# USAID Target Enterprise Information Architecture

# System Concept Report

*Prepared by*

**Computer Sciences Corporation**

**1100 Wilson Boulevard**

**Arlington, VA 22209**

*February 2000*

**Document No: 06 004**

USAID
PRIME
Principal Resource for
Information Management Enterprise-wide

USAID

## Table of Contents


1. Introduction ..... 1
2. The Business of USAID ..... 2
   2.1 Mission Statement ..... 2
   2.2 The Core Business of USAID ..... 2
   2.3 Standard Business Model ..... 2
   2.4 Strategic Drivers ..... 3
   2.5 Collocation With Department of State ..... 3
   2.6 USAID Washington ..... 3
   2.7 USAID Missions ..... 6
   2.8 USAID Partners ..... 7
3. USAID's Business Processes ..... 7
4. Applicable Government Requirements ..... 9
5. The Year 2000 Baseline Architecture ..... 11
6. Motivation for Improving USAID's Enterprise Information Architecture ..... 13
7. Goals of the Target Enterprise Information Architecture ..... 15
   7.1 Vision Statement ..... 15
   7.2 Goals of the Target Enterprise Information Architecture ..... 15
8. Operations Concept ..... 17
9. Applications, Data, Security, and Technical Architecture ..... 22
   9.1 USAID/W Application and Data Architecture ..... 22
   9.2 Technical Infrastructure ..... 29
   9.3 Mission Application and Data Architecture ..... 34
   9.4 Security Architecture ..... 38
      9.4.1 Network Security Mechanisms ..... 41
      9.4.2 Server Workstation Security Mechanisms ..... 41
      9.4.3 Client Workstation Security Mechanisms Client ..... 42
      9.4.4 Application Software and Data Security Mechanisms ..... 42
   9.5 External Interfaces ..... 43
10. Conclusion ..... 44
11. Abbreviations and Acronyms ..... 46

12. References ..... 51
Appendix A. Federal Enterprise Architecture Conceptual Framework ..... A-1
Appendix B. Raines' Rules ..... B-1
Appendix C. Example Process Scenarios ..... C-1
C.1 Acquisition Scenarios ..... C-1
C.2 Property Management Scenarios ..... C-2
C.3 Summary ..... C-4
Appendix D. Legend for Architecture Diagrams ..... D-1
Appendix E. External Interface Summary Table ..... E-1

## List of Tables

Table 2-1. Information Technology Strategic Drivers ..... 4
Table 2-2. Mapping of TEIA To Reform Roadmap Systems ..... 4
Table 4-1. Key Provisions of the Clinger-Cohen Act ..... 10
Table 8-1. Evaluation of Mission Operations Concept Options ..... 21
Table 9-1. Implementation Options ..... 26
Table 9-2. Required Security Services and Their Implementing Mechanisms ..... 39

## List of Figures

Figure 2-1. USAID Standard Business Model ..... 3
Figure 2-2. USAID Operating Units ..... 5
Figure 2-3. Mission Staff Size ..... 7
Figure 3-1. Business Areas Supported by the TEIA ..... 9
Figure 8-1. Distributed Mission Operations Concept ..... 17
Figure 8-2. Centralized Mission Operations Concept ..... 18
Figure 8-3. Hybrid Mission Operations Concept ..... 19
Figure 9-1. IFMS 3-Tier Architecture ..... 22

Figure 9-2. USAID/W IFMS Option 1 ..... 23
Figure 9-3. USAID/W IFMS Option 2 ..... 24
Figure 9-4. USAID/W Knowledge Management ..... 27
Figure 9-5. Development Community Virtual Workspace ..... 28
Figure 9-6. USAID/W Local Area Network ..... 29
Figure 9-7. USAID/W Wide Area Network Interfaces ..... 30
Figure 9-8. Mission LAN Architecture and WAN Interfaces ..... 30
Figure 9-9. Commercial WAN Infrastructure Options ..... 32
Figure 9-10. USAID/W Applications (IFMS Option 1), Data, Network Architecture ..... 33
Figure 9-11. USAID/W Applications (IFMS Option 2), Data, Network Architecture ..... 34
Figure 9-12. Mission Thin Client Option ..... 35
Figure 9-13. Mission Desktop Database Option ..... 36
Figure 9-14. Mission Data Server Option ..... 37
Figure 9-15. USAID/W Security Architecture ..... 40
Figure 9-16. Mission Security Architecture ..... 41

# 1. Introduction

Various studies have documented USAID's inability to perform essential accounting and reporting functions according to U.S. Government standards. USAID is unable to conform to Office of Management and Budget (OMB) guidelines and legislative mandates, experiences high operations and maintenance costs, and has inconsistent data because of the lack of modern integrated enterprise information systems. In addition, USAID's current information systems provide only limited support to core business areas of economic and humanitarian assistance.

This is the second of three reports that document options for a target Enterprise Information Architecture (TEIA) that will enable USAID to meet critical business requirements. The following paragraphs describe the three reports. High-level agency planning anticipates that the transition to this TEIA will be complete in the time period 2002-2004.

The *USAID Target Enterprise Information Architecture System Requirements Report* defines complete, consistent, and feasible system requirements that satisfy business needs and specify the target system. It organizes and summarizes functional, data, performance, security, and operational system requirements. The functional and data requirements represent reengineered business processes planned to improve USAID's operations. System developers detail the requirements during subsequent development phase design activities.

The *USAID Target Enterprise Information Architecture System Concept Report* describes the current information systems architecture and identifies agency motivation and goals for changes to information systems. It includes a vision for a TEIA and alternatives for a realization of that vision that meets agency goals. The report defines operations concepts for using the system to execute business processes.

The *USAID Target Enterprise Information Architecture System Design Report* develops and evaluates system architecture alternatives and then selects one system architecture as the baseline. It specifies numbers and sizes of technical components necessary to meet the system requirements. The baseline system architecture is the foundation upon which subsequent development phase design activities build.

Taken together, these three reports, coupled with the *USAID Y2K Baseline Architecture Report,* fulfill the mandate of the CIO Council's *Federal Enterprise Architecture Conceptual Framework.* Appendix A gives a detailed mapping of these documents to the eight components of the framework.

# 2. The Business of USAID

The purpose of USAID's information systems is to enable the agency to perform its core business functions. This section provides an overview of the business of USAID at a level necessary to interpret the TEIA.

## *2.1 Mission Statement*

USAID contributes to U.S. national interests through the results it delivers by supporting the people of developing and transitional countries in their efforts to achieve enduring economic and social progress and to participate more fully in resolving the problems of their countries and the world.

*-USAID Strategic Plan, September 1997*

## *2.2 The Core Business of USAID*

The core business of USAID is to produce sustainable development in developing and transitional countries. USAID directs a $7 billion annual program of economic and humanitarian assistance to more than 100 countries in the developing world, Central and Eastern Europe, and the former Soviet Union. The agency achieves its core business goals by planning, carrying out, and assessing results of programs for

- Economic growth and agriculture development
- Human capacity development
- World population stabilization and human health protection
- World environment protection
- Open political institutions/democracy
- Humanitarian assistance

## *2.3 Standard Business Model*

Figure 2-1 shows the business model USAID uses to achieve these objectives. The agency achieves its core business goals through transfer of knowledge and capital to its customers in the form of technical and training services, goods, and financial resources, either directly or through intermediary partners.

Congressional legislation, results of performance on development goals, and goals from the *USAID Strategic Plan* are the drivers for planning, implementing, and managing agreements with partners who deliver aid in these developing countries. The performance metrics from the partners serve as feedback in monitoring the agreements. External sources (e.g., the World Health Organization (WHO) and the United Nations Children's Fund (UNICEF)) provide performance results that measure the agency's success in reaching its development goals.

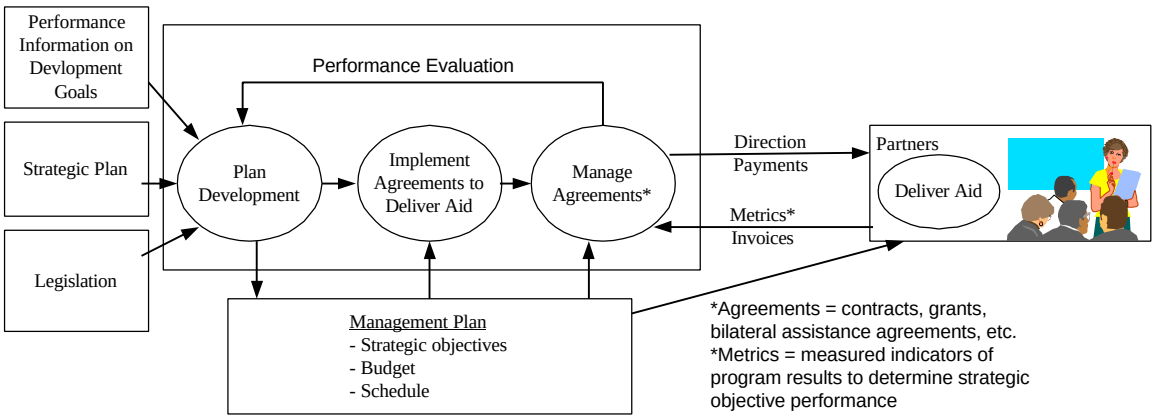



**Figure 2-1. USAID Standard Business Model**

## *2.4 Strategic Drivers*

The *USAID Strategic Plan* is a guide for achievement of USAID's mission. One of the goals listed in the *USAID Strategic Plan* is that "USAID remains a premier development agency." Under this management goal, the agency identifies a number of approaches that are tactics to achieve its mission. The *USAID Strategic Plan*, Annex 1, USAID Management Objectives, details the approaches that are drivers for the modernization of the USAID information systems; Table 2-1 lists them.

In response to the strategic plan, USAID defined a *Reform Roadmap* to focus on the way work is performed and to look for ways to perform work more efficiently. *Annex A* provides an action plan in four broad areas, one of which is *Agency-Wide Systems*. Elements of the TEIA provide capabilities, discussed below, to support each of the seven systems identified in the plan. Table 2-2 maps the elements of the TEIA to the reform roadmap systems.

## *2.5 Collocation With Department of State*

Concern about the increased threat to the physical security of United States Government facilities and employees has lead to planning within USAID for collocation of some missions with Department of State facilities. This allows them to share a common physical security perimeter. This collocation provides the opportunity to improve the cost-effectiveness of USAID information systems by sharing communications and administrative services. Therefore, where consistent with achieving USAID's goals, the TEIA should be designed and implemented for ease and efficiency of operations within Department of State facilities.

## *2.6 USAID Washington*

USAID is headquartered (USAID/W, Figure 2-2) in the Ronald Reagan Building (RRB) in Washington, D.C., and currently maintains missions in approximately 80 countries. The total workforce of USAID employees is approximately 7,000. In Washington, D.C.,

USAID has a staff of approximately 1,500 employees, comprising 1,100 civil service employees and 400 foreign service employees.

**Table 2-1. Information Technology Strategic Drivers**

| Program Approach Number | Program Approach | Need That Drives Information System Modernization |
|---|---|---|
| 1.1.1 | Emphasis on effective field presence continued | Integrated information systems in the missions to provide improved efficiency and effectiveness in managing development programs |
| 1.1.2 | Strategic partnering with U.S.-based and local non-governmental organizations enhanced | Procurement flexibility and monitoring of contract/award progress and results<br>Collaborative computing and sharing of knowledge assets |
| 1.2.3 | Performance goals more precisely stated, annual monitoring of performance results against goals improved, and commitment to using evaluations to identify "Best Practices" and to sharing these within USAID and among development partners renewed | Program planning, results tracking, and knowledge systems |
| 1.3.3 | Sustainable development results documented | Results tracking and knowledge systems |
| 1.4.2 | Workforce planning improved | Human resource systems and integration with program planning and budgeting systems |
| 1.4.3 | Results reporting and financial management systems enhanced | Data integration and reporting for all financial and mixed financial systems |

**Table 2-2. Mapping of TEIA To Reform Roadmap Systems**

| Action Plan System | TEIA Element |
|---|---|
| Managing for results | Project management (supported by financial management) |
| Funds allocation | Budget |
| Acquisition and assistance | Procurement |
| Funds accounting system | Financial management |
| Workforce management system | Human resources |
| Information management system | Technical architecture<br>Security architecture<br>Financial management, Procurement, Budget, Project management |
| Automated directives system | Document management |

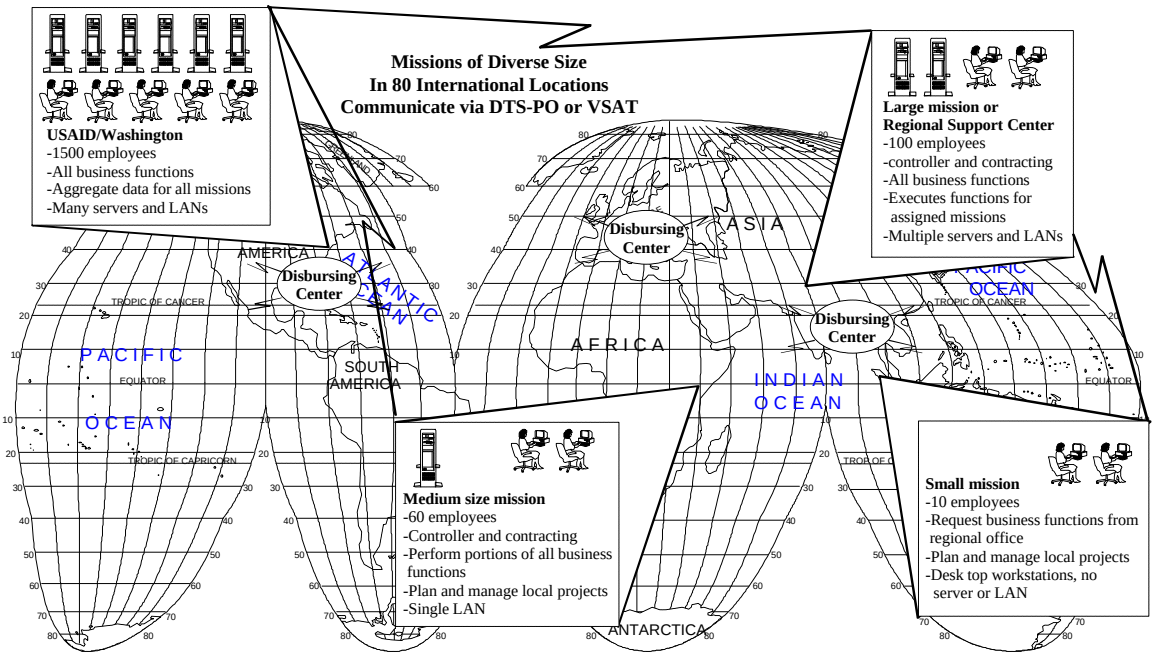



**Figure 2-2. USAID Operating Units**

USAID's organizational structure comprises regional bureaus and central bureaus. The regional bureaus administer the missions, while central bureaus provide functional policy guidance to mission staff.

The four regional bureaus are the Bureau for Europe and Eurasia (E&E), Bureau for Latin America and the Caribbean (LAC), Bureau for Africa (AFR), and Bureau for Asia and the Near East (ANE). Each regional bureau guides and coordinates its regional missions to identify the needs of people in the host country and assess the country's commitment to sustainable progress.

USAID has five central bureaus. The Bureau for Humanitarian Response (BHR) fields programs for disaster assistance and Food for Peace (a joint program with the Department of Agriculture). The Bureau for Global Programs, Field Support, and Research (G) programs address the health, population, nutrition, environment, democracy and governance, economic growth, and other areas crucial to the agency's programmatic goals. Some central programs are administered directly from Washington without the involvement of the missions.

Other central bureaus provide services to the agency either in Washington or at a mission. The Bureau for Policy and Program Coordination (PPC) includes among its policy and planning responsibilities the collection and evaluation of program results and development information. The Bureau for Management (M) conducts agency financial and mixed financial business support services and maintains the agency's core information systems. The Bureau for Legislative and Public Affairs (LPA) provides the agency's channel for interaction with Congress.

The agency also has offices reporting to the administrator. These include Office of the Executive Secretariat (ES), Office of Equal Opportunity Programs (EOP), Office of Small and Disadvantaged Business Utilization/Minority Resources Center (OSDBU/MRC), Office of the Inspector General (IG) and Office of the General Counsel (GC).

## *2.7 USAID Missions*

Each of the missions USAID maintains develops a strategic plan for the host country to address some or all of USAID's core business goals. The country program is consistent with the *USAID Strategic Plan* and complementary to the worldwide program. Each mission implements programs to achieve the goals of its host country strategic plan.

In response to the Government Performance and Results Act (GPRA), many operating units embraced the use of result-oriented teams and reorganized around those teams, while the official central personnel structure remained in a traditional hierarchy. The reengineering of processes focussed on enhancing the efficiency and authority of the field operations by increasing delegation of authority and reducing required clearances. This effort was designed to allow missions, which were seen as a strength of the agency, to manage for results and improve program efficiency.

Although the missions have been USAID's comparative advantage within the development community, diminishing operational resources are forcing the agency to consider alternative ways of supporting its programs. One possibility is the consolidation of agency business resources and infrastructure around a limited number of standardized regional support centers. This approach would place most business support functions at regional support centers, while program operations would continue to be performed at smaller client sites in the countries of the region, where program staff could work directly with partner and customer representatives as they do now. Missions vary significantly in size, staffing, and functionality. (See Figure 2-3). The large regional support center missions have more than 100 employees and a full complement of staff from the central bureaus. They execute all business functions for their mission and other missions. They have the need and support capability for one or several LANs with multiple servers and local server administration.

Medium-size missions have approximately 60 employees, including a complement of staff from the central bureaus. They execute portions of all business functions for their missions. The predominant function of a mission is to plan and manage local projects. Mission information systems typically consist of a single local area network (LAN) with one or a few servers and minimal local system administration.

Small missions have about 10 employees, most or all of who plan and manage local projects. They execute requests for business services to either regional support centers or USAID/W. Employees at small missions generally have desktop workstations. They may have no LAN or local system administration.

The missions all communicate with USAID/W or with other missions over a wide area network comprised of VSATs and DTS-PO communications links. Section 5 discusses these communications systems.

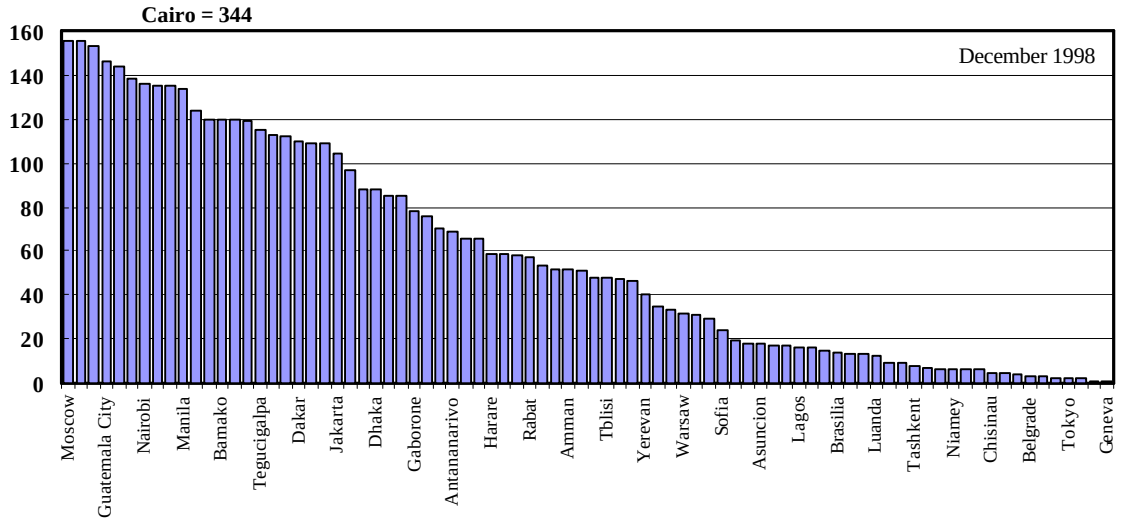



**Figure 2-3. Mission Staff Size**

### *2.8 USAID Partners*

To further the use and the effectiveness of in-country development teams and to leverage additional resources to be focussed on the agency's goals, USAID pursues its goals through partnerships. USAID depends on the partners to execute most programs. Partnerships are with the people and governments of the host government, non-governmental organizations (NGOs), private voluntary organizations (PVOs), academic institutions, other United States Government agencies, and international assistance agencies, including international financial institutions, multilateral and bilateral donors, and private foundations.

In cooperation with these partners, USAID identifies the needs of the host country, assesses the country's commitment to sustainable progress, and develops country-specific plans. At the country level, USAID seeks to build strategic partnerships that facilitate local resource mobilization and action; encourage local participation and advocacy for development and humanitarian efforts; and foster cooperation among local actors. At the international level, USAID's efforts contribute to building a consensus among bilateral and multilateral donors on the key problems of sustainable development.

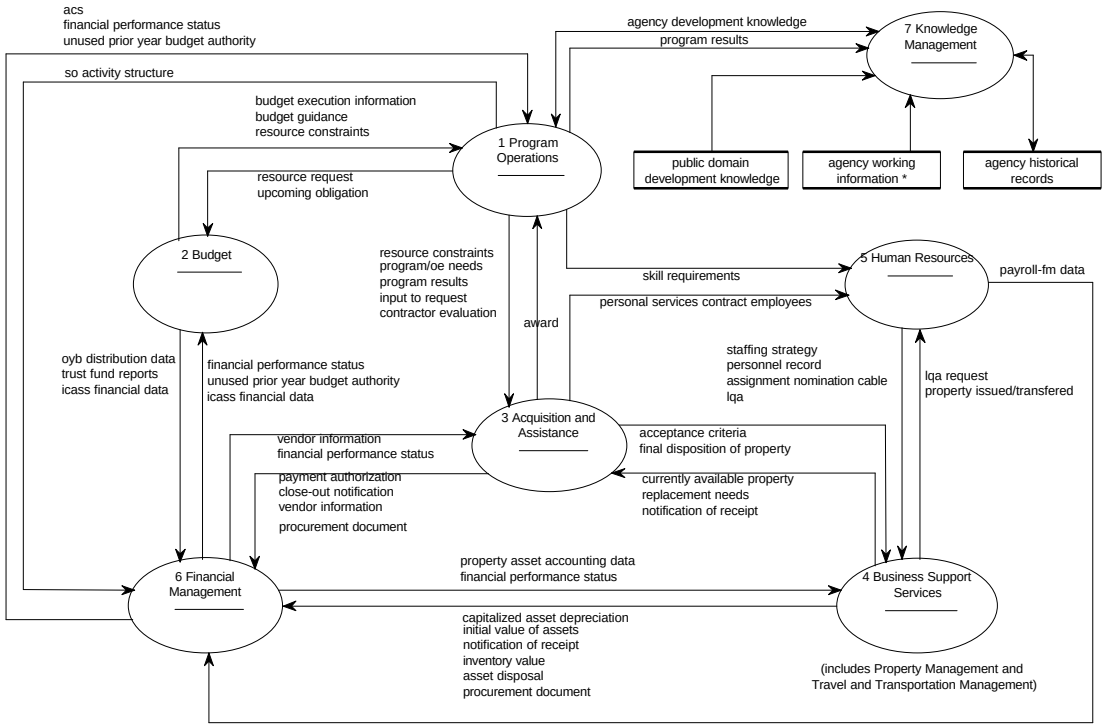
## 3. USAID's Business Processes

The TEIA provides the functionality to support USAID's business processes for budgeting, planning, procurement, monitoring contracts and awards, and tracking results. The business processes also encompass the administrative functions of financial and personnel management. Information systems performing these functions are classified as

mixed financial systems and fall under the requirements of the *Chief Financial Officers Act* and the *Federal Managers Financial Integrity Act* (FMFIA). Because USAID depends on partners to deliver most development aid to recipients, the TEIA does not support delivery processes directly.

Figure 3-1 illustrates the business process areas the TEIA is to support. (The process names used in the list reflect common commercial usage. USAID specific terminology for the process areas is included in parentheses and the figure where applicable.)

- Financial Management–Core accounting functions of general ledger, accounts payable, accounts receivable, funds management, and cost accounting.
- Budget–Formulation of budgets, justification for presentation to Congress and OMB, and execution of the approved budgets.
- Procurement (acquisition and assistance)–Purchase of goods and services and administration of contracts and grants.
- Human Resources–Workforce planning, recruitment, personnel management, training, labor relations, benefits administration, and payroll.
- Business support services – including travel and transportation management; and property management of both real and personal property, where personal property includes both expendable and non-expendable property.
- Knowledge Management–Electronic storage, retrieval, and collaborative creation of documents and historical records comprising the knowledge assets of USAID/W, agency missions, and development partners.
- Program Management (program operations)–Planning development programs, scheduling the activities and resources, and tracking results from the programs.




* agency working information = data from current agency operations and business activities (including data flows on this diagram and those internal to the business areas)

**Figure 3-1. Business Areas Supported by the TEIA**

# 4. Applicable Government Requirements

Although there are numerous relevant regulatory requirements from different government agencies, they can be traced, in large part, to the *Information Technology Management Reform Act* (also called the *Clinger-Cohen Act*). This legislation specifies the basic requirements for the direction in which USAID needs to go with its information systems and how it needs to get there.

The *Clinger-Cohen Act* is the primary source of regulatory requirements placed on investments in information systems by U.S. Government agencies. The Act's primary purposes are to streamline information system acquisitions and emphasize life-cycle management of information systems as a capital investment.

Table 4-1 summarizes provisions of the *Clinger-Cohen Act* that are particularly significant for decision-making in support of the USAID TEIA. The information in Table 4-1 is drawn from the Government Accounting Office (GAO) web site.

This TEIA has been developed to enable USAID to comply with these regulatory requirements. The TEIA is a direct result of analyzing the agency's mission and business processes and provides a blueprint for future investment decision making (CCA 5123(5)). The TEIA enables USAID to identify individual investment modules (CCA 5222), assess their relative value, and manage their risks (CCA 5122) on a consistent enterprise-wide

basis. Once identified, these investments can be integrated with other agency planning processes (CCA 5122(b)2).

**Table 4-1. Key Provisions of the Clinger-Cohen Act**

| Reference | Provision |
|---|---|
| CCA 5122 | Agency heads are to design and implement a process for maximizing value and assessing and managing risks of their IT acquisitions, to provide for the selection of investments using<br>• Minimum criteria that include quantitatively expressed, projected net-risk-adjusted return on investment<br>• Specific quantitative and qualitative criteria for comparing and prioritizing alternative information system projects |
| CCA 5122(b)2 | The IT investment process of executive agencies is to be integrated with the processes for making budget, financial, and program management decisions. |
| CCA 5123(3) | Agency heads shall ensure that performance measurements are prescribed for IT used by or to be acquired for the agency and that the performance measurements measure how well the IT supports agency programs. |
| CCA 5123(5) | Agency heads are to analyze the agency's missions and, based on the analysis, revise the agency's mission-related and administrative processes (as appropriate) before making significant investments in IT used to support those missions. |
| CCA 5222 | The head of the agency should, to the maximum extent practicable, use modular contracting for the acquisition of major information technology systems:<br>• Successive acquisition of interoperable increments complying with common or commercially accepted IT standards<br>• Award of contracts within 180 days after the date on which a solicitation is issued<br>• Delivery of the information technology within 18 months after the date on which the solicitation resulting in award of the contract was issued |

## 5. The Year 2000 Baseline Architecture

The RRB in Washington, D.C., is the main headquarters for USAID and provides access to centralized computing resources and network connectivity. Banyan Vines is the primary network operating system (NOS), providing file and print services to all Banyan Vines users. Banyan Vines' enterprise-wide StreetTalk Directory Services are the basis for the agency's email systems. Banyan Vines NOS does not directly support application services, so applications residing on Banyan Vines servers require only network connectivity for operation. None interface directly with the Banyan Vines operating system.

Windows NT servers also provide file and print services to RRB users. They are not as widely used as Banyan Vines for this function, however. The agency has exploited the versatility of Windows NT at the RRB by using it to provide both infrastructure and application support in those areas not supported by Banyan. A single Windows NT domain has been created for RRB users, and it is used to enforce desktop policies during Banyan logins and to serve as a distribution control point for desktop virus signature updates. Both solutions reduce visits to the desktop client. Examples of Windows NT applications at USAID include some Web servers and all Lotus Notes servers.

The core financial system used at the agency, the New Management System (NMS), supports four business process areas: financial management, budget, acquisition and assistance, and program operations. NMS resides on an IBM RS/6000 Advanced Interactive Executive (AIX) Unix host. NMS is a two-tier client-server application that uses Oracle as the database management system. Client requests are submitted to Oracle in the form of SQL statements, and data is returned for client processing and presentation. The Windows 95 desktop NMS client uses this information and implements the business logic of the application. NMS is currently only active in USAID/W but was designed with a remote distributed processing environment in mind.

The RRB also supports Sun Solaris hosts, another implementation of Unix. They are used to provide network services and to address system management roles. The network management system and problem management hosts are both examples of this. In addition, one critical application, Mission Accounting and Control System (MACS), also operates on a Solaris host.

The LAN in the RRB consists of a 100 Mbps switched Ethernet backbone and provides the connections to the core backbone switches. The backbone infrastructure includes Cisco routers and switches, with 10/100 Mbps interfaces for connections to local workstations. Network traffic consists of Vines IP, transmission control protocol/internet protocol (TCP/IP), and NetBEUI protocols. This traffic is logically segmented into broadcast domains by using use Cisco's implementation of virtual LANs (VLANs).

Within the Washington, D.C., metropolitan area, USAID has three sites that are connected by public telephone communication links. One is the Technology Hub (TechHub) in Rosslyn, Virginia, which is connected via a fiber-optic distributed data interface (FDDI) network service (FNS) connection. The TechHub is a contractor site used primarily as a facility for NMS developers and PRIME personnel. Although its infrastructure is similar to the RRB, it does not host any operational USAID applications.

USAID maintains a small administrative office in Springfield, Virginia, connected to the RRB via a 56 kbps line.

The third site is the USAID Data Center, SA-26, located in a Department of State facility in Beltsville, MD. An FNS communications link is installed between RRB and SA-26 and is used to transmit TCP/IP traffic. In addition to this connection to the RRB, there is a T-1 connection that carries non-TCP/IP traffic.

The Beltsville facility houses an IBM mainframe and executes both MVS/ESA and OS/390 on the same physical system. The two OSs are kept logically isolated from each other by using logical partitions on the mainframe. The mainframe hosts two of the agency's mission-critical legacy applications: the New American Payroll System (NAPS) and the Revised Automated Manpower & Personnel System (RAMPS).

NAPS is the legacy payroll application, and RAMPS is the application used to manage other human resources information. Both applications require support from Banyan Vines for terminal access and report printing and distribution. Connectivity to the RRB is implemented by using the T-1 connection to carry synchronous data link control (SDLC) traffic. SNA gateways are used to connect the mainframe to the Banyan network.

Beltsville also supports two Wang VS minicomputers (VS300 and VS7310). The Wang computers are likely to be retired from operations in the near future.

USAID foreign missions also use Banyan Vines for email, print, and file services but have deployed other solutions as well. Hardware platforms and software packages are more diverse at the missions to accommodate the assorted projects found there. The missions all communicate with USAID/W or with other missions over a wide area network (WAN) comprised of very small aperture terminals (VSATs) and Diplomatic Telecommunication System–Program Office (DTS-PO) communications links.

The Department of State provides the DTS-PO consolidated telecommunications service to approximately 270 embassies and consulates in 160 countries and to other federal agencies with foreign operations, e.g., the U.S. Department of Agriculture’s (USDA's) Foreign Agricultural Service (FAS) and Commerce's International Trade Administration (ITA). As many as 40-50 federal agencies have foreign offices and are eligible to receive telecommunication services through the DTS-PO, and USAID makes widespread use of this eligibility. DTS-PO uses an encrypted X.25 telecommunications protocol to support transmission of both classified and sensitive but unclassified (SBU) information. DTS-PO lines from the Department of State terminate in both the RRB and the Beltsville facility. Maximum bandwidth for DTS-PO connections is 64 kbps.

VSAT operations rely on satellite technology for TCP/IP communications. There are two VSAT hubs, one located in Goonhilly, England, and one in Whitsenville, Massachusetts. Missions utilize either the Goonhilly site or the Whitensville site but not both. Bandwidths for each site are asymmetrical. The Whitensville outroute channel is 512 kbps. Goonhilly has a 128 kbps outroute channel and a 1 Mbps outroute channel. Inroute channels are 128 kbps for both sites. Not all missions have VSAT capabilities.

External access to the internal network is protected by network firewalls. Firewalls permit email and attachments to enter the USAID/W LAN but prevent any other attempts to access network resources from the outside. USAID firewall policies also prevent non-HTTP traffic from reaching the public web site.

## 6. Motivation for Improving USAID's Enterprise Information Architecture

Reviews of the agency's financial management systems reveal that their capability to provide reports that conform to current legislation is weak and deficient. These findings, summarized below, are noted in the following reports: the *Inspector General's Audit of USAID's Progress Implementing a Financial Management System That Meets Federal Management Improvement Act Requirements* and the *Review of Material Weaknesses Reported in FY 1998 Federal Managers Financial Integrity Act Report*.

USAID lacks adequate and complete information to file regulatory reports that comply with OMB Circular A-127, the *Chief Financial Officers Act of 1990,* and OMB Budget Bulletin No. 93-02. The agency's accounting systems do not comply with applicable federal accounting standards, required under FMFIA, including the ability to post transactions to the U.S. Standard General Ledger and the structured classification of financial information. This limits USAID's ability to provide financial reporting with understandable, relevant, and reliable information about financial position, activities, and operations results.

In addition, USAID's core financial systems do not meet Joint Financial Management Improvement Program (JFMIP) requirements to support the *Prompt Payment Act.* NMS-generated reports are not timely, accurate, or sufficiently useful to manage the agency's business. NMS's financial management component does not consistently produce reliable obligation and expenditure information. Data migration of active and historical information on agency business encounters substantial difficulties.

Furthermore, USAID financial and mixed-financial systems are not integrated to the degree required by JFMIP. All modules must access the same data entered at a single point in the system. The current system's lack of integration compromises controls and agency information integrity.

Internal controls are compromised by the agency's inability to ensure prevention and timely detection of unauthorized acquisition, use, or disposition of assets. As a result, the agency is not complying with such laws as the *Accounting and Auditing Act of 1950,*

which established requirements for an effective internal control system, and the *Federal Managers Financial Integrity Act of 1982*, which reinforced the need for effective internal controls. By implementing these controls, USAID would ensure that resource use is consistent with laws, regulations, and policies; resources are safeguarded against waste, loss, and misuse; and reliable data are obtained, maintained, and disclosed in reports.

USAID's systems do not comply with the requirements of the *Computer Security Act*. As a result, systems could be jeopardized by unauthorized data modification, destruction of computer resources, disruption of operations, and compromise or loss of resources that include agency-sensitive information.

Finally, USAID lacks any significant information systems support for operations planning and management. Operations planning and management require collaborative efforts between USAID staff and development partners and the sharing of knowledge gained in previous engagements or as the product of research.

Eliminating these deficiencies in USAID's business processes requires replacement of the supporting information systems. This replacement will be consistent with the TEIA defined in this report. Replacement of current systems with the TEIA is compliant with OMB Circular A-11 eight guidance rules for information system investments. Appendix B gives the complete text of the rules The paraphrasing of the rules is for reference only.

Rule 1: Support core/priority functions

All business process functions within the scope defined in Section 3 are required for the agency to perform its mission.

Rule 2: No alternative private sector or governmental source

A cross-servicing assessment will be performed before each implementation phase. The TEIA does not presume or preclude alternative sources.

Rule 3: Redesigned work processes to make maximum use of commercial-off-the-shelf technology

Preliminary process redesign has been performed for all work areas. Commercial-off-the-shelf (COTS) products are highly leveraged in the TEIA and are expected to provide the bulk of the applications and data structures. Detailed processes will be defined when each product is selected to ensure that product capabilities are leveraged with minimum customization. This is expected to result in significant process redesign.

Rule 4: Return on investment

USAID is unable to function successfully and comply with Federal laws and regulations with current systems. Eliminating these deficiencies justifies the investment. Specific product selections will include return on investment analysis.

Rule 5: Consistent with information architecture

The projected architecture will leverage modern information system investments and replace obsolete or high-cost technology. The information architecture will be

built to accommodate the core financial and mixed financial product performance requirements.

Rule 6: Reduce risks by avoiding custom components
COTS products are highly leveraged in the TEIA and are expected to provide the bulk of the applications and data structures. Prototypes and capability demonstrations will be used where necessary.

Rule 7: Be implemented in phased, successive chunks
The TEIA will be implemented in phases fully compliant with this rule.

Rule 8: Allocate risk between government and contractor
The PRIME contract, which will be used to implement the modernization, is compliant with this rule.

# 7. Goals of the Target Enterprise Information Architecture

USAID has defined a TEIA vision that, when achieved, will provide the business functionality required to support accomplishment of the agency's mission.

## *7.1 Vision Statement*

USAID information management systems provide every employee access to the tools and information at his/her workstation necessary to carry out the agency's mission with the highest level of responsible stewardship of federal resources. The systems promote information sharing and collaboration with USAID international development partners to achieve shared strategic objectives (SOs).

## *7.2 Goals of the Target Enterprise Information Architecture*

The TEIA should support the achievement of *USAID Strategic Plan* goals and objectives in a manner that is cost effective and consistent with sound accountability standards and in compliance with applicable regulations. The information system strategic drivers listed Table 2-1 lead to the following goals for the TEIA:

- Financial management capability that provides managers worldwide with complete, reliable, timely, and consistent information enabling them to monitor and report on assets, liabilities, revenues, obligations, expenditures, and the full cost of programs
- Agency-wide resource planning capability that meets the requirements of all related U.S. Government laws and regulations
- A secure system that ensures the suitability and security of USAID associates, information, and physical environment without inhibiting achievement of agency goals
- Support for the dynamic changes occurring in the agency
- Improved system functional and performance capabilities at reduced cost by using commercial products and practices to the maximum extent

- Capability for the systems to support all authorized users in planning, implementing, and evaluating the agency's business (ease of access to information in every operating unit)

The first two goals are closely related. The financial management capability is required to enable USAID to effectively manage programs and resources. The laws and regulations establish that requirement and provide related guidance on how to meet the requirement. Security is an essential technical feature of the architecture to enable the systems to accomplish their functions successfully. An effective security architecture is also required by Government laws and regulations.

USAID is an agency with an inherently dynamic business environment. As the development and disaster assistance needs of countries change with time, USAID must reassign staff and resources, resize missions, open new missions, and close old missions. Changes in Government funding and initiatives to reinvent Government business processes result in a decreasing staff at USAID to perform core business functions. Increased threats to Americans in foreign locations require USAID to respond. (Section 0 discusses an example.).

The architecture must provide the flexibility and increased productivity to enable USAID to function successfully within the context of these changes. It must accomplish this in a manner that facilitates USAID's ability to achieve its mission.

The architecture must make effective use of commercial products and practices to reduce system and operating costs while improving efficiency. Products must be selected for ease of integration and maintenance in addition to meeting functional and performance needs. Therefore, the product with the best functional or performance capabilities may not be selected for a given function. If another product provides lesser but adequate capabilities but is more easily integrated or maintained, it may be selected over the product with superior capabilities

Similarly, USAID may have to alter business processes or procedures if, by doing so, it reduces the cost or risk of implementing a new product. Generally, the most costly and risky approach is to modify commercial products to adapt them to existing processes. Developing custom software, when commercial products are available, has a similar set of risks and costs. Developing interfaces between commercial products has yet another set of costs and risks. The best commercial practice is to adapt processes to the capabilities of the product that integrates most easily with the other elements of the enterprise architecture.

Another strategy for improving system functionality while reducing cost is simplifying the architecture. This is accomplished by providing modern system management capabilities and standardizing desktop applications, operating systems, mail systems, and communications protocols.

# 8. Operations Concept

The key operations concept question for the target architecture is how the missions interact with USAID/W or a regional support center. There are three options for this interaction to support the wide variation in mission size and capability. Each mission chooses an operations concept that meets its business needs and technical capabilities. As these change over time, each mission decides whether to change from one concept to another. At any point in time, a number of missions employ each of the three concepts. At any point in time, a number of missions employ each of the three concepts. Appendix C presents example scenarios that reflect the roles of individuals in executing a portion of an agency business process. The scenarios highlight both the similarities and differences associated with process execution for the three mission operations concepts.

Figure 8-1 illustrates the distributed operations concept. This concept reflects an extension of the way medium and large missions operate today. Each mission functions as an independent business unit with a full set of mission-specific data and applications. This option minimizes dependence on USAID/W for daily operations. It gives the mission staff the full range of capabilities to execute transactions and manage all of their business processes and data. They query the data to generate new or standard reports in any format that they find productive to use. If the mission is also a regional support center, it performs all or some business functions for assigned smaller missions.

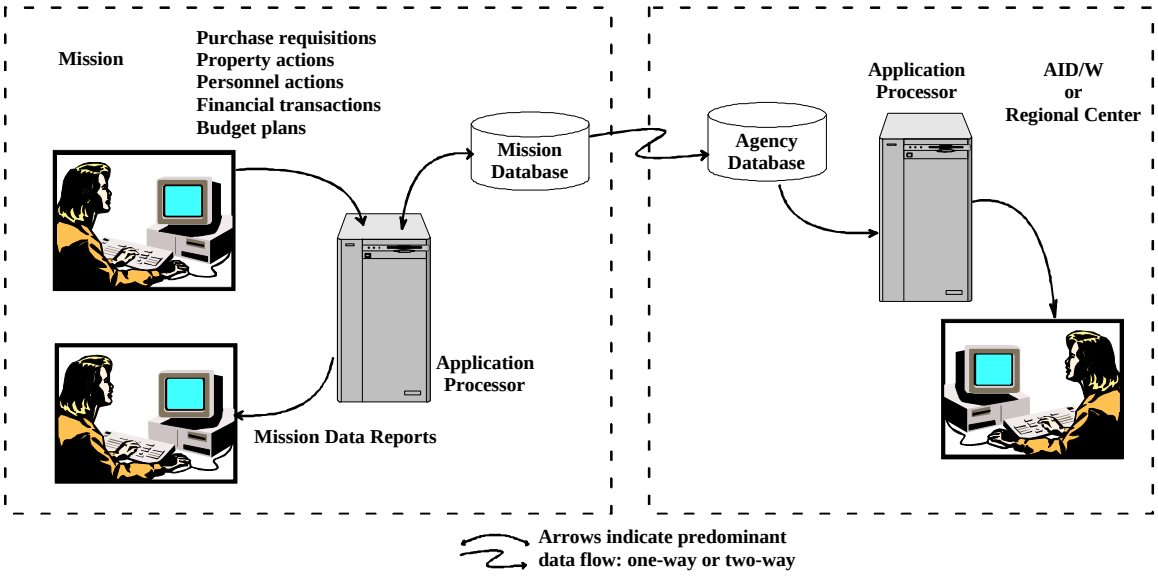



**Figure 8-1. Distributed Mission Operations Concept**

USAID/W obtains the mission's data, including all data fields for each integrated financial management system (IFMS) transaction, through one of a variety of mechanisms, including database replication, flat file transmission, email attachment, or physical medium transfer. Data on each USAID/W-initiated transaction are similarly

transferred from USAID/W to the mission, along with such items as budget guidance and e-mail.

Because transactions for a mission may be entered either in the mission database or in the USAID/W database, this concept requires significant attention to synchronizing data between USAID/W and the missions. Each transaction entered in a mission must be copied to the USAID/W database. Each mission-related transaction entered in USAID/W must be copied to its respective mission database. This two-way synchronization is complex and risky to implement, especially across unreliable communications links.

The existence of two copies of the operational database raises potential end user problems as well. As an example, if the same funds are obligated for different purposes in a mission and USAID/W, the conflict must be resolved by using automated or operational mechanisms. One operational approach is to divide the mission's funds into two subsets, one to be obligated by the mission and one to be obligated by USAID/W.

It also requires attention to assuring that updates to the application software are synchronized. The IFMS software packages are large and complex. It is essential that every patch or upgrade be deployed to all sites hosting the software. The logistics and testing requirements are expensive to implement and difficult to manage across a global organization. It may place demands on the WAN that cannot be met with infrastructure available in the host country. The effort associated with synchronizing data and applications adds costs and risks the integrity of the data.

Figure 8-2 illustrates the centralized operations concept. This concept represents the standard operations concept the IFMS vendors recommend for geographically dispersed enterprises. The users in each mission access their data stored on USAID/W data servers over the WAN. The performance of the WAN is such that the user's productivity is not degraded by comparison to a local user in Washington. Security mechanisms prevent users from accessing data for missions they are not authorized to support.

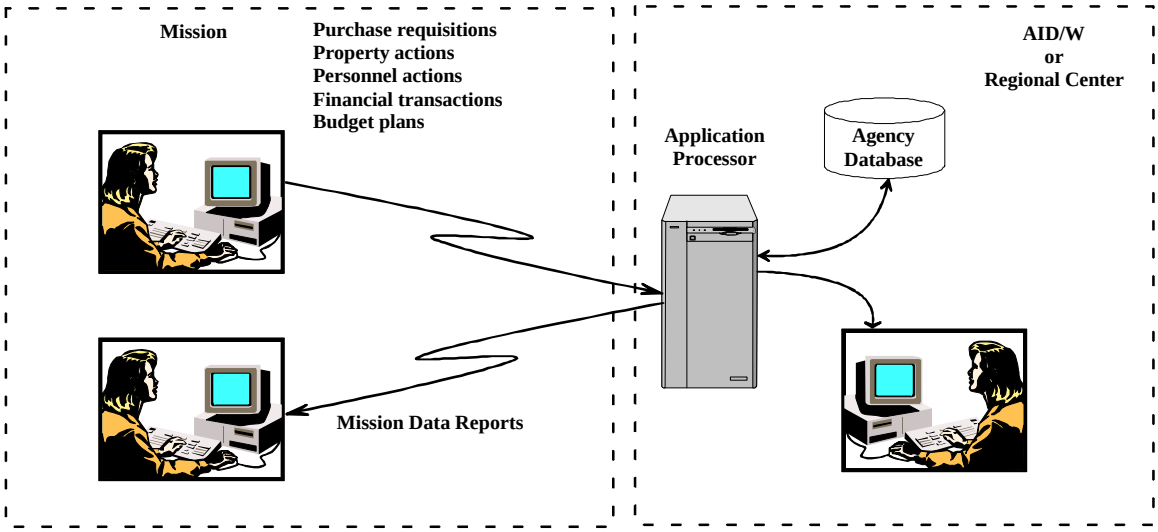



**Figure 8-2. Centralized Mission Operations Concept**

Users in the mission also have access to all the IFMS applications on servers located in USAID/W. This option gives the mission staff full capabilities to execute transactions and manage all of their business processes and data. They query the data to generate new or standard reports in a format that they find productive to use. If the mission is also a regional support center, it performs all or some business functions for assigned smaller missions.

Because the data for all missions is stored in a single database instance in USAID/W, there are no concerns about data synchronization. Because the applications are stored on servers in USAID/W, there is no concern about multiple site application maintenance. Wherever a mission can obtain adequate communication links back to USAID/W, this is the preferred operations concept. However, because USAID requires mission operations in underdeveloped nations, many missions are unable to obtain adequate communication links to USAID/W for this option to work successfully. Even in locations where the communications are available, the cost must be weighed against the benefits of this concept as compared to the third concept.

Figure 8-3 illustrates the hybrid operations concept. It incorporates the distributed execution of transactions with the centralized database. Users in missions have data entry capabilities to enable them to execute any required business process. Local workflow capabilities enable multiple users in a mission to participate in or approve transactions such as obligations. Once the mission's portion of the workflow is complete, the data for each IFMS transaction are transferred to USAID/W.

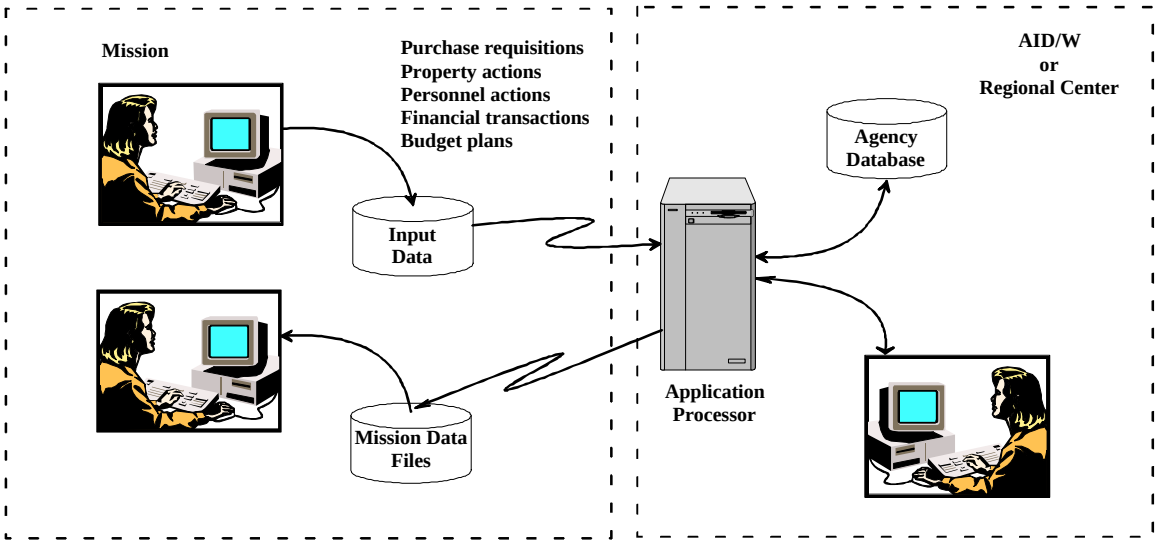



**Figure 8-3. Hybrid Mission Operations Concept**

Transactions become final when they are entered into the USAID/W database. Transactions may also be rejected. For example, a transaction would be rejected if it attempted to obligate funds that had previously been obligated by someone else. Because the final acceptance of all transactions takes place in a single location, there is no automated conflict resolution. The user is notified of completion or rejection of each transaction. This process eliminates the need to synchronize two databases.

Data reflecting the status of each mission's business processes, plus such items as budget guidance, are extracted from the USAID/W data server in flat file form and transmitted or shipped on physical media to the mission. Users in the mission query the data to generate new or standard reports in a format that they find productive to use. They do not have the capability to modify the data in USAID/W except via the data entry process discussed in the preceding paragraph. The level of detail and timeliness of the mission's data is directly related to its communications capabilities with USAID/W.

This concept results in the highest dependency of the missions on either a regional support center or USAID/W. They face potential performance risks because they do not have full control over all steps in core business processes. However, the risks and costs of data and application synchronization are much less than with the distributed operations concept. This option has the least dependence on WAN performance and so minimizes the operations risks in countries without a modern communications infrastructure.

Each of the three mission operations concepts has its advantages and disadvantages summarized in Table 8-1. The distributed option has minimal dependence on host country and USAID/W infrastructure, and provides the mission staff with full capability to manage all business processes and data. However, it entails costs and risks associated with data and software synchronization.

The centralized concept depends heavily on host country and USAID/W infrastructure. It provides the mission staff with full capability to manage all business processes and data, and minimizes risks and costs of data and software synchronization. The hybrid option results in an intermediate assessment on all criteria.

Based on this assessment, the USAID uses the following criteria to select a system concept for a mission. The centralized mission operations concept is selected whenever high-speed, low-latency, reliable, affordable wide area network (WAN) communications with USAID/W or the regional center are available. When this capability is not available, the distributed concept is selected so long as there is capable system administration staff and a large transaction volume at the mission. If capable system administration staff are not available or the transaction volume is not large, the hybrid concept is selected.

**Table 8-1. Evaluation of Mission Operations Concept Options**

| | Mission Operations Concept Option | | |
|---|---|---|---|
| Criterion | Distributed | Centralized | Hybrid |
| Dependence on host country WAN infrastructure | + | - | x |
| Dependence on USAID/W for daily operations | + | - | x |
| Mission staff have full capability to manage all business processes and data | + | + | x |
| Data synchronization risk & cost | - | + | x |
| Multiple site application maintenance risks and cost | - | + | x |

+ = Positive assessment in trade-off of risk, cost, and capability
x = Neutral assessment in trade-off of risk, cost, and capability
- = Negative assessment in trade-off of risk, cost, and capability

# 9. Applications, Data, Security, and Technical Architecture

## *9.1 USAID/W Application and Data Architecture*

The application and data architecture is built around two COTS product suites: the IFMS products and the knowledge management products. The IFMS products provide all the functionality required by the business processes discussed in Section 3 except for knowledge management. The following paragraphs discuss IFMS and knowledge management separately.

The leading IFMS product vendors designed their products to be configured in a three-tier centralized architecture (depicted in Figure 9-1). The central database is the core of the IFMS software design. It contains all data necessary for the functionality and operation of the products, including the mapping of privileges to roles and roles to users.

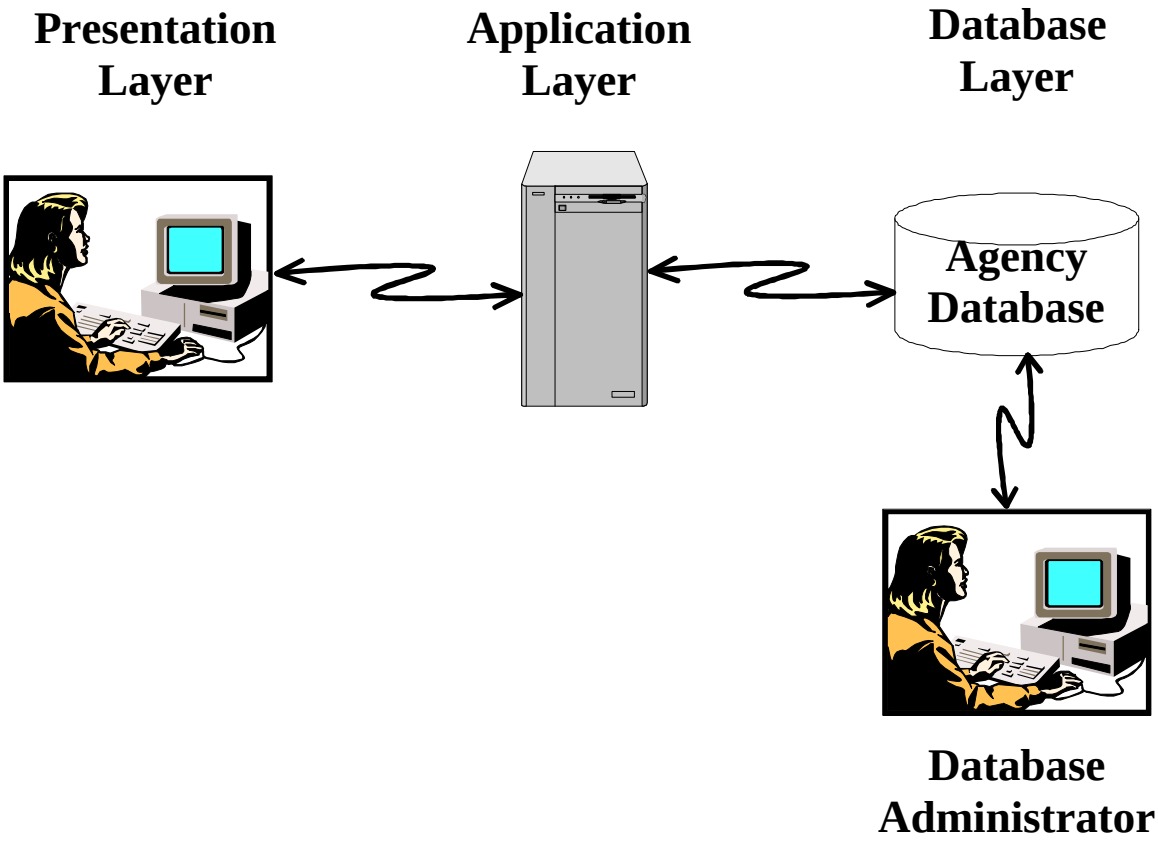



**Figure 9-1. IFMS 3-Tier Architecture**

Users access the system from desktop workstations that host an IFMS application presentation layer. The presentation layer displays data requested from the application server and enables users to input data to the application server. Users generally have no direct access to the database unless granted special privileges. Only database administrators have regular direct access to the database.

The standard configuration employs a single instance of the central database. A single database instance eliminates significant complexity introduced in synchronizing data in multiple database instances. Some vendors integrate all the data into a single database, as Figure 9-2 shows for USAID/W. (Appendix D provides a legend for interpreting the symbols in the architecture diagrams.) Others employ separate databases, shown in Figure 9-3 for major functional areas, and integrate the overlapping data (e.g., payroll payments with general ledger) using scheduled transactions.

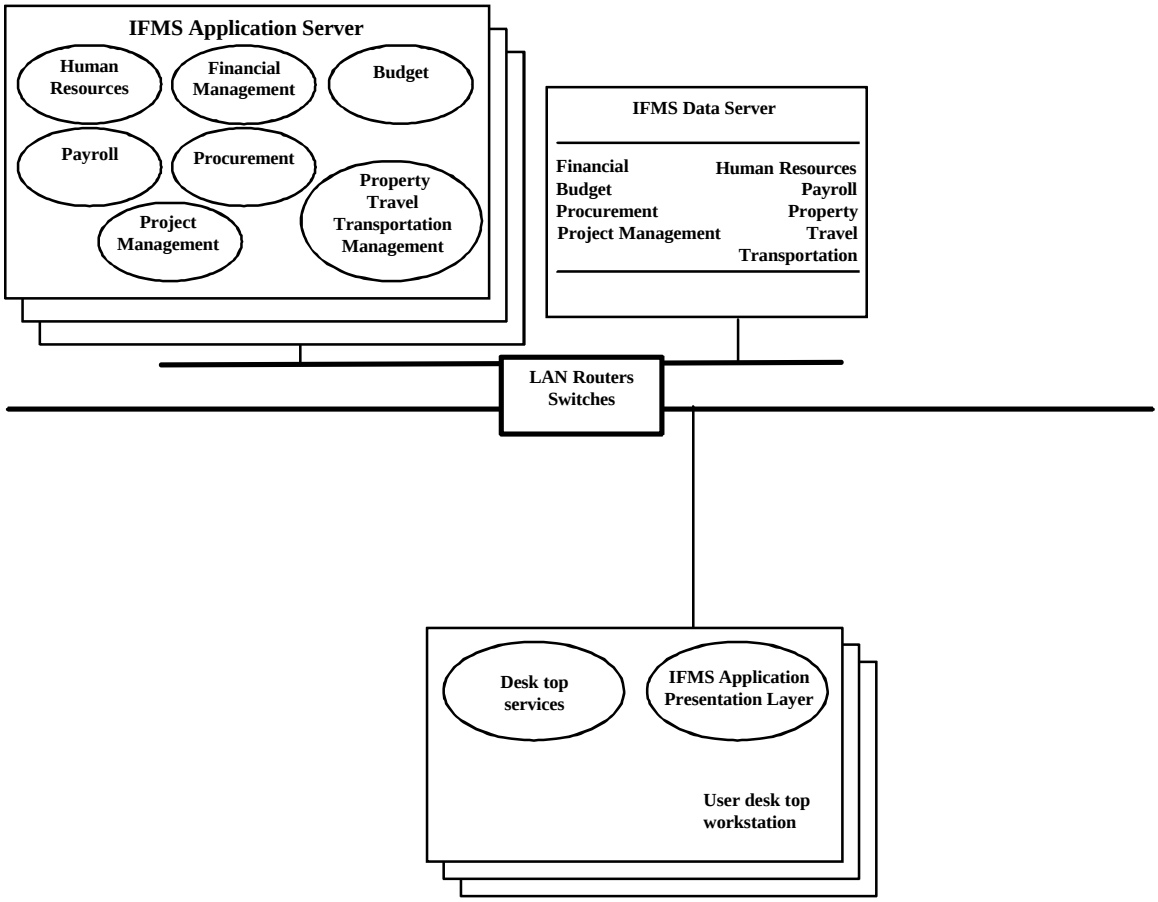



**Figure 9-2. USAID/W IFMS Option 1**

The central database is preferably hosted on a single data server to simplify system and database administration. When database size or demand exceed the capability of a single data server, multiple clustered data servers may be used to host the central database. In this configuration, there is still a single logical central database, but it is spread across multiple physical data servers. Built into the design of the single database instance and

data server must be adequate backup and redundancy to meet availability requirements of the agency and to protect against equipment failure.

For USAID, the central database contains data from all the missions and for USAID/W operating units to enable all accounts to be accumulated into agency-wide totals. The only users who require access to this full set of data are those in the USAID/W operating units. Locating this database in the RRB or in a nearby Washington, D.C., metropolitan area location obviates the need for expensive long-distance communication links between the users in USAID/W operating units and the central database.

The PRIME contractor maintains and operates the central database for USAID. The PRIME maintains most of its staff in the Washington area, which has a large pool of information system workers. Therefore, maintenance and operation of the central database is feasible in this location. This is in contrast to many USAID mission locations where it is difficult to hire local skilled information system workers.

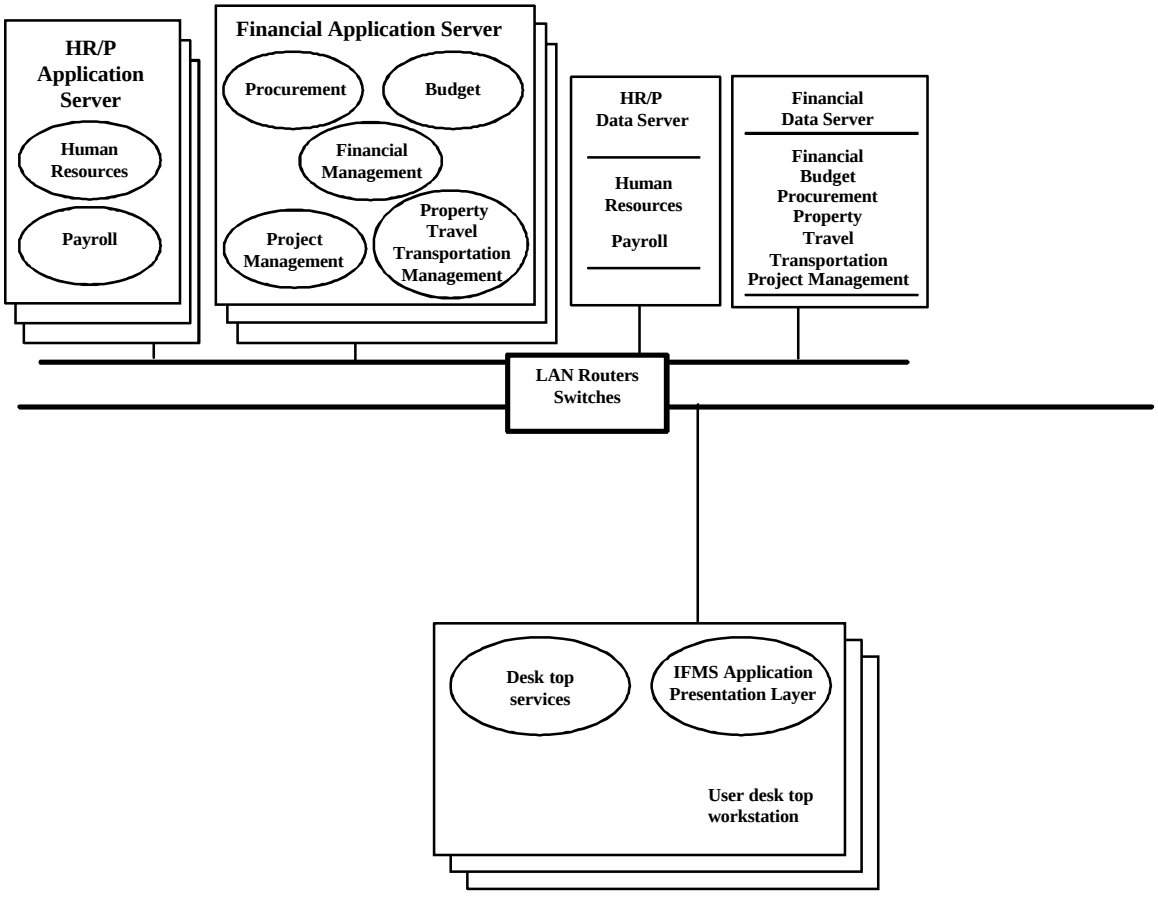



**Figure 9-3. USAID/W IFMS Option 2**

The standard configuration for the IFMS application server employs one instance of each application on one or a small number of powerful application servers. Maintaining a single or small number of instances of each application minimizes both the cost of maintaining the applications and the risk that users will inadvertently be using different

versions or configurations of applications. Vendors formerly distributed the applications to the users' desktop. While it is feasible to host applications on the user desktop, it has no advantages in a multi-user environment and is strongly discouraged by the vendors.

Multiple application servers are used when there are a large number of users and demand exceeds the capability of a single server. Multiple application servers are also used when there is a desire to decouple server demand for different major functional areas. An example is the potential conflict for resources between closing the general ledger and issuing paychecks.

Multiple application servers are also a mechanism for maintaining availability. If two servers are adequate for meeting user demand, three servers can be deployed. When all servers are running, users find they have excess resources, and their needs are well met. When one of the application servers fails, the users assigned to that server are shifted to the two remaining servers. Resources are then reduced but remain adequate, and user needs are still met.

Some vendors provide all their applications in a single package that must be hosted on all application servers. Other vendors provide independent modules that can be hosted on either a single server, as Figure 9-2 depicts, or separate servers, as Figure 9-3 depicts. It is also technically feasible to host the applications on the data server. However, this places high demand on server resources and complicates server management. Co-hosting the applications and data is advisable only in an environment with a small number of users and is not advisable for USAID/W.

The IFMS applications require frequent high-volume access to the database. Therefore, the application servers must be collocated with the data server on a dedicated LAN segment.

Each user of the system has an instance of the IFMS application presentation layer on his/her desktop workstation. The presentation layer provides a graphical user interface (GUI) to the applications, which in turn access the database. The vendor implementations of the GUI (Table 9-1) are either native to the operating environment on the desktop (Windows, Macintosh, Unix), Internet browsers or are electronic forms. The user desktop workstation also provides standard office services, including a word processor, spreadsheet, Internet browser, and other required single user applications.

USAID/W local users communicate with the IFMS applications server over a high-speed LAN (10-100 Mbps). Remote users are discussed later in this report.

Figure 9-4 depicts the knowledge management application and data architecture. Groupware products provide a suite of capabilities to meet the knowledge management requirements defined in the *USAID Target Enterprise Information Architecture System Requirements Report*. These products include messaging, directory, document management, and collaborative computing capabilities. The document management capabilities are used for USAID's knowledge assets as well as records management and correspondence tracking.

**Table 9-1. Implementation Options**

| Architecture Element | Options |
|---|---|
| IFMS Application Presentation Layer | Vendor Windows<br>Internet browser<br>Groupware forms<br>Spreadsheet, word processor<br>Custom |
| IFMS Mission Database | Copy of AID/W mission database<br>Flat file export of AID/W mission data<br>Spreadsheet, word processor |
| IFMS Single User Applications | Vendor applications<br>Spreadsheet, word processor<br>Custom |
| Groupware client | Vendor client<br>Internet browser |
| Data communications | Real-time over high speed network<br>Asynchronous file transfer<br>Replication<br>E-mail attachment<br>Physical media transfer |

Separate knowledge management groupware servers are provided for use by USAID's development partners to share knowledge assets and work collaboratively in planning and executing development and assistance programs. Internet servers supplement groupware functionality.

The combined capability of groupware and Internet services comprises a virtual workspace for the development community. As Figure 9-5 illustrates, users at USAID/W, missions, and development partners all have access to the USAID/W knowledge management servers. The servers are managed by the PRIME contractor and contain contributions from individuals throughout the development community. Missions and development partners may also host knowledge management servers with their own contributions to the virtual workspace.

Security mechanisms in the servers and firewalls assure that authorized users have access to required data while the data is protected from all other users. These mechanisms provide adequate trust because they are based on the use of cryptographic keys distributed by a USAID/W certificate server. Public keys for all users are distributed through the directory services. This enables users to encrypt data to be sent to any other user over the public Internet without concern for the privacy or integrity of that data. Only the recipient has the private key necessary to decrypt the data.

Each user desktop workstation hosts an instance of the groupware client software. The groupware client may provide the forms interface to the IFMS application server. The leading groupware vendors are implementing new interfaces that may require only an Internet browser on the user desktop workstation. The IFMS product may use the groupware messaging capability to trigger user action in workflow processing.

The groupware server software is hosted on a knowledge management groupware server, along with the data. Multiple knowledge management groupware servers are required to serve the demands of USAID users. Built-in data replication capabilities synchronize the data across multiple servers. To protect the integrity of valuable USAID data, data are replicated from internal servers to the development partner servers. No data are replicated automatically from the development partner servers to the internal servers. Any data transfers require human intervention. The knowledge management groupware server communicates with the groupware client over the same LAN used by user to access the IFMS.

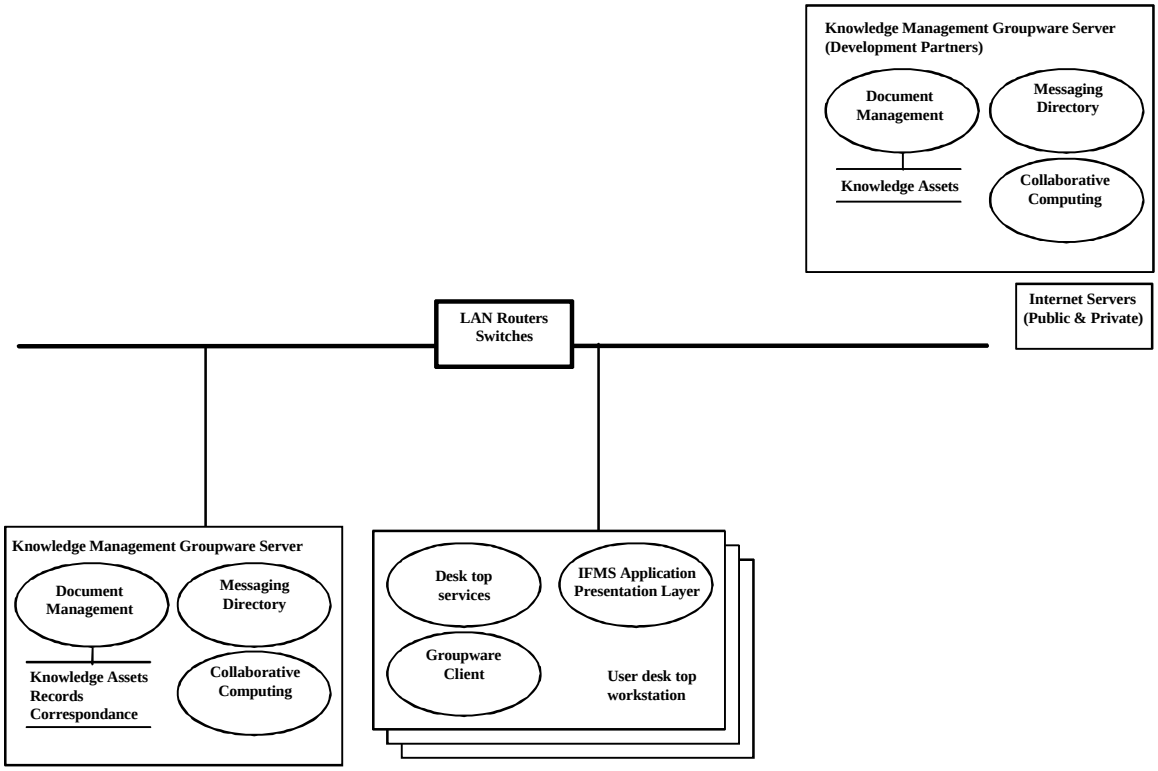



**Figure 9-4. USAID/W Knowledge Management**

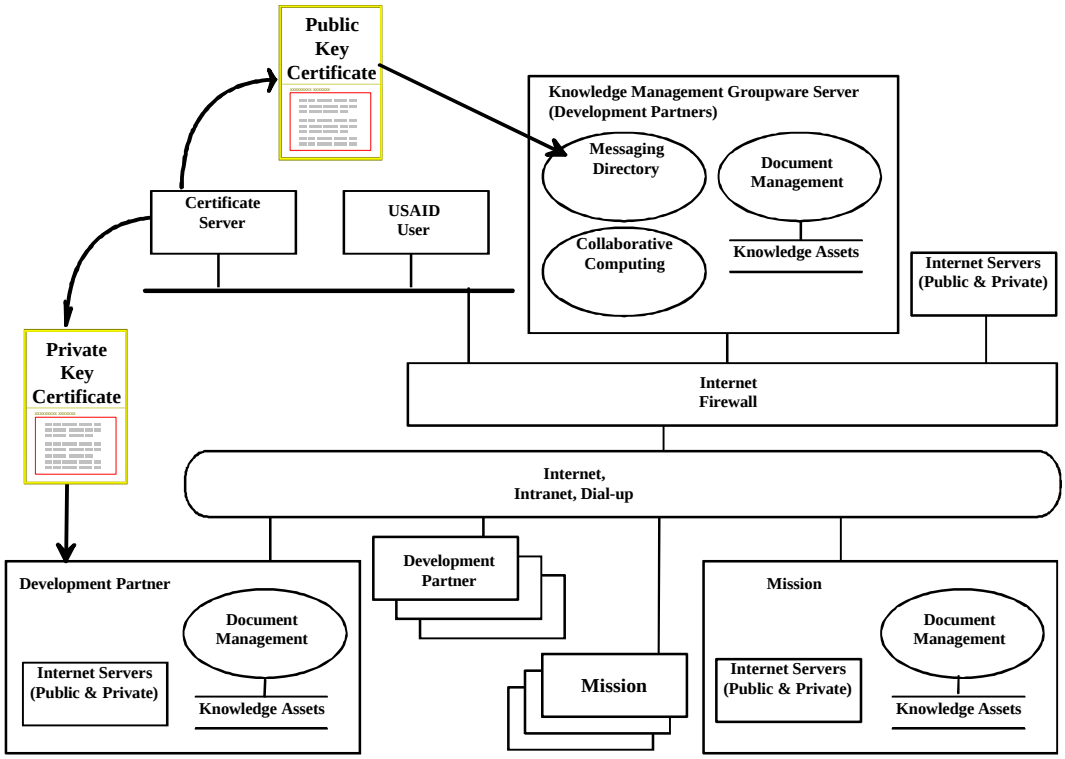



**Figure 9-5. Development Community Virtual Workspace**

## *9.2 Technical Infrastructure*

The technical infrastructure comprises the server and client computers, OSs, and networks (local and wide area).

The IFMS application and data servers are selected on the basis of recommendations by the product vendors. They either host Unix or Windows 2000 OSs. (Note: Windows NT 5.0 has been renamed Windows 2000.) All other servers in the system host Windows 2000 OSs to minimize the complexity and cost of managing the system. User desktop workstations are a Windows 95/98 or Windows 2000 client. The computers are selected to be compatible with the operating system and performance requirements.

In USAID/W, the LAN, shown in Figure 9-6, employs 100 Mbps Ethernet at the data link layer, IP at the network layer, TCP at the transport layer, and standard internet application layer protocols. Routers and switches divide the network into subnetworks as required for efficient communications. A domain name server provides network directory and naming services. Networked printers provide print services. Network servers provide scan, file, database, and directory services.

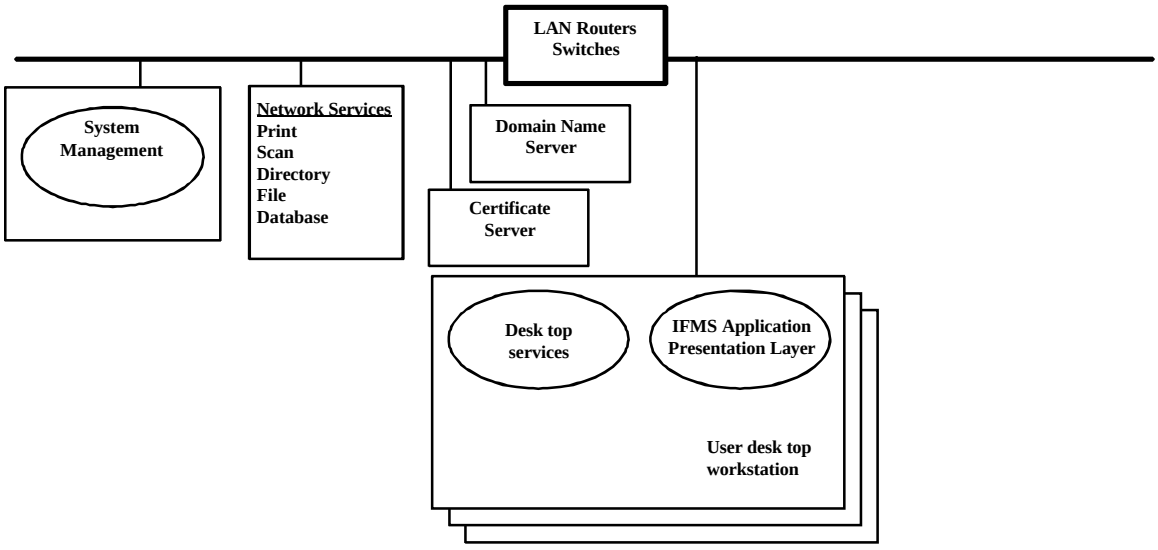



**Figure 9-6. USAID/W Local Area Network**

A system management server contains configuration management, performance management, fault management, and security management components. The configuration management component controls the devices connected to the network and distributes software. The performance management component monitors the throughput and responsiveness of devices connected to the network. The fault management component detects, isolates, and records faults and executes or supports response to return service to nominal levels. The security management component controls all security mechanisms.

USAID/W has the only certificate server to provide a single trusted source for cryptographic keys. Public keys are distributed using directory services so users have no need to access the certificate server directly except to receive their private key. Consequently, there is no significant network impact introduced by having only one in Washington for the entire agency.

WAN services are necessary to connect USAID/W to missions, development partners, other Government agencies, the PRIME contractor, and the public. Figure 9-7 depicts USAID/W WAN interfaces.

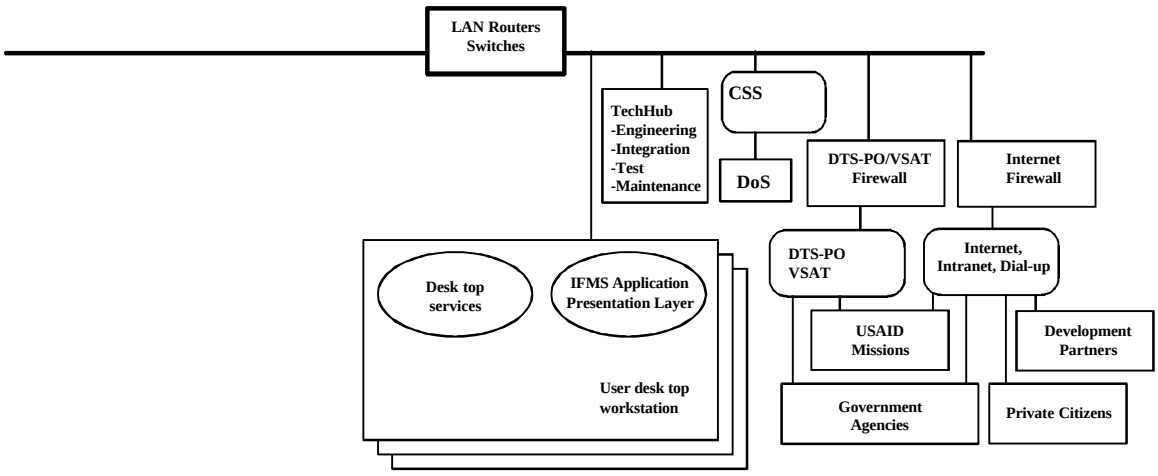



**Figure 9-7. USAID/W Wide Area Network Interfaces**

Missions deploy a technical architecture comprised of a subset of the USAID/W technical architecture. Figure 9-8 depicts the full set of potential mission technical architecture elements. Individual missions implement those elements consistent with business needs and system administration staff capabilities. Missions work closely with embassies and other Department of State facilities and are frequently located near to or collocated with them. Direct connectivity to the Department of State facilitates that interaction.

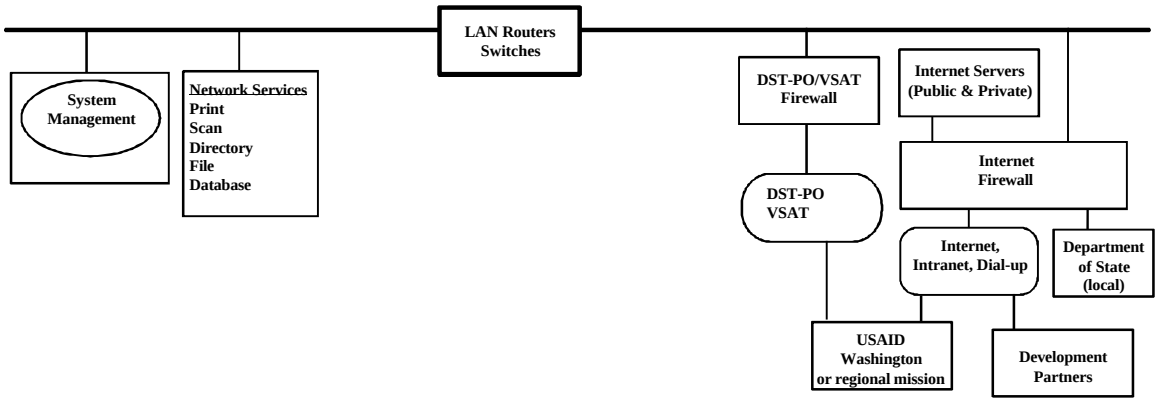



**Figure 9-8. Mission LAN Architecture and WAN Interfaces**

Print and scan services are local to each mission. Missions with good communication links to USAID/W depend on USAID/W or a regional support center for system management, file access, and domain name services. Missions with poor communication links perform these functions locally consistent with their capabilities.

Missions that are too small to support local system administration staff and that have poor communication links to USAID/W do not deploy servers. They perform all functions on user desktop workstations. Each individual is assigned a workstation with all required capabilities. Connection to other USAID sites is made directly from the workstation via a variety of mechanisms.

A global WAN links the missions to each other and to USAID/W as required. DTS-PO and leased VSAT services provide current WAN communications. USAID has a mandate to use DTS-PO for international WAN services. All foreign service agencies are required by law to obtain wide area communications services from DTS-PO for facilities located in foreign countries, unless DTS-PO is unable to meet the communications requirements. USAID currently has a waiver that allows use of the VSAT network as a backup to DTS-PO. The current DTS-PO and VSAT networks are described in the *USAID Y2K Baseline Architecture Report*.

Where DTS-PO does not provide adequate service to a mission, USAID continues to use the VSAT or constructs another intranet from available local services that include telephone dialup, leased circuits, the Internet, or satellite-based service. As communications capabilities are deployed by commercial entities, new options become available for improved mission communications. Because of the wide variation of available services, USAID will not have a homogeneous WAN for the foreseeable future.

Figure 9-9 illustrates some of the commercial WAN infrastructure capabilities available in cities where USAID missions are located (December 1998 locations). High-speed T1 and frame relay service is available in many mission locations. A fiber-optic cable running from Portugal to Malaysia along the west coast of Africa will expand service in 2002 to additional cities with missions. Internet service providers in many cities provide an additional option for communications within the USAID community and access to the public Internet. The communications provider and service is determined individually for each mission based on a cost vs. benefit trade-off among available telecommunications options.

All WAN interfaces providing access to USAID operating unit information systems are protected by firewalls discussed in Section 9.4, Security Architecture. USAID's communication links to other Government agencies and development partners are designed on a case-by-case basis. USAID has a direct connection to the Department of State through the Cable Switching System (CSS). USAID also needs to provide information to the public on its mission and operations. As Internet access becomes reliable and effective in foreign locations, USAID leverages those capabilities. Servers accessed over the public Internet provide public information.

Figure 9-10 and Figure 9-11 depict integrated USAID/W applications, data, and network architectures.

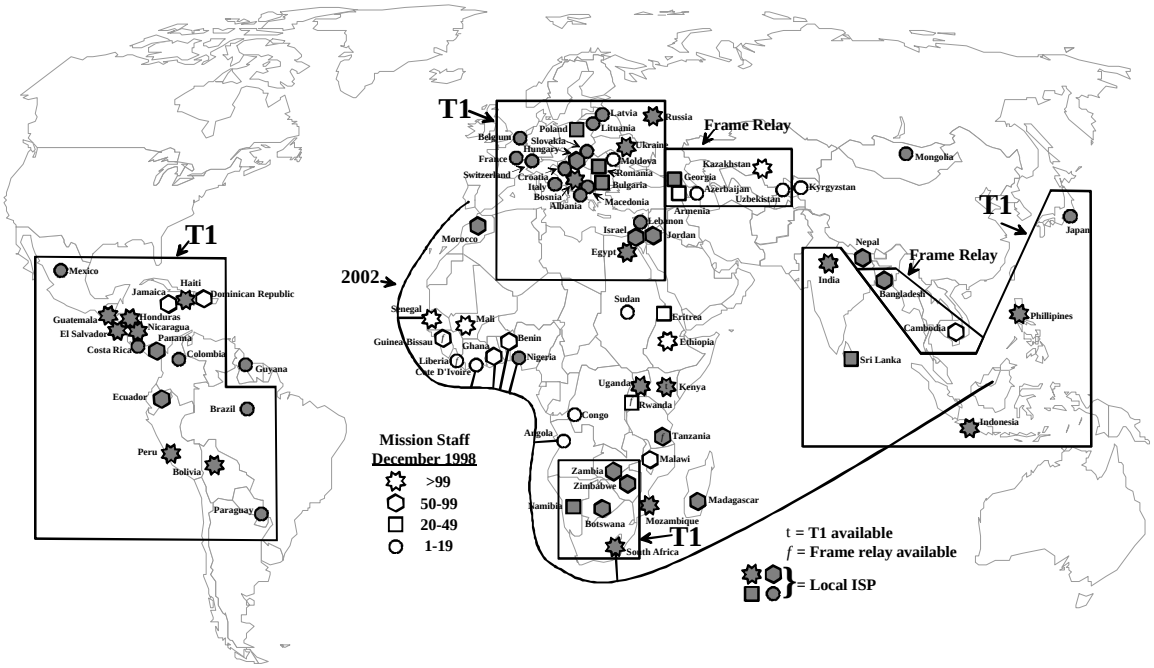



**Figure 9-9. Commercial WAN Infrastructure Options**

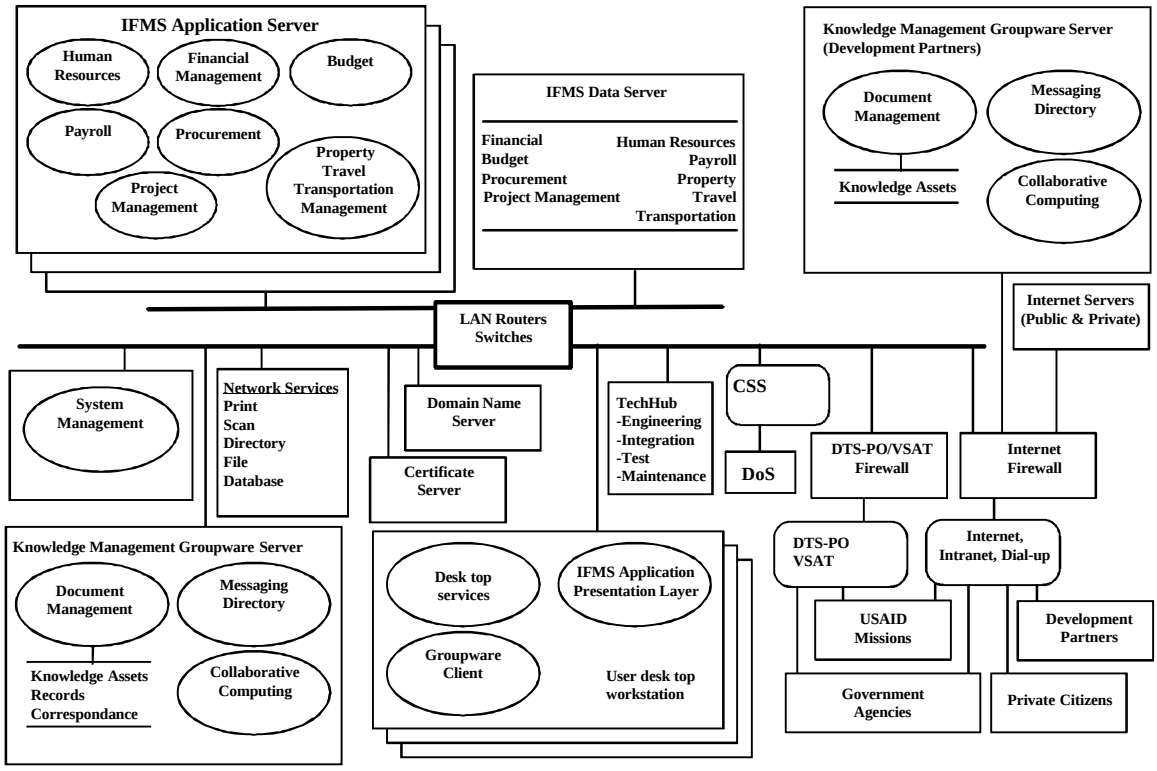



**Figure 9-10. USAID/W Applications (IFMS Option 1), Data, Network Architecture**

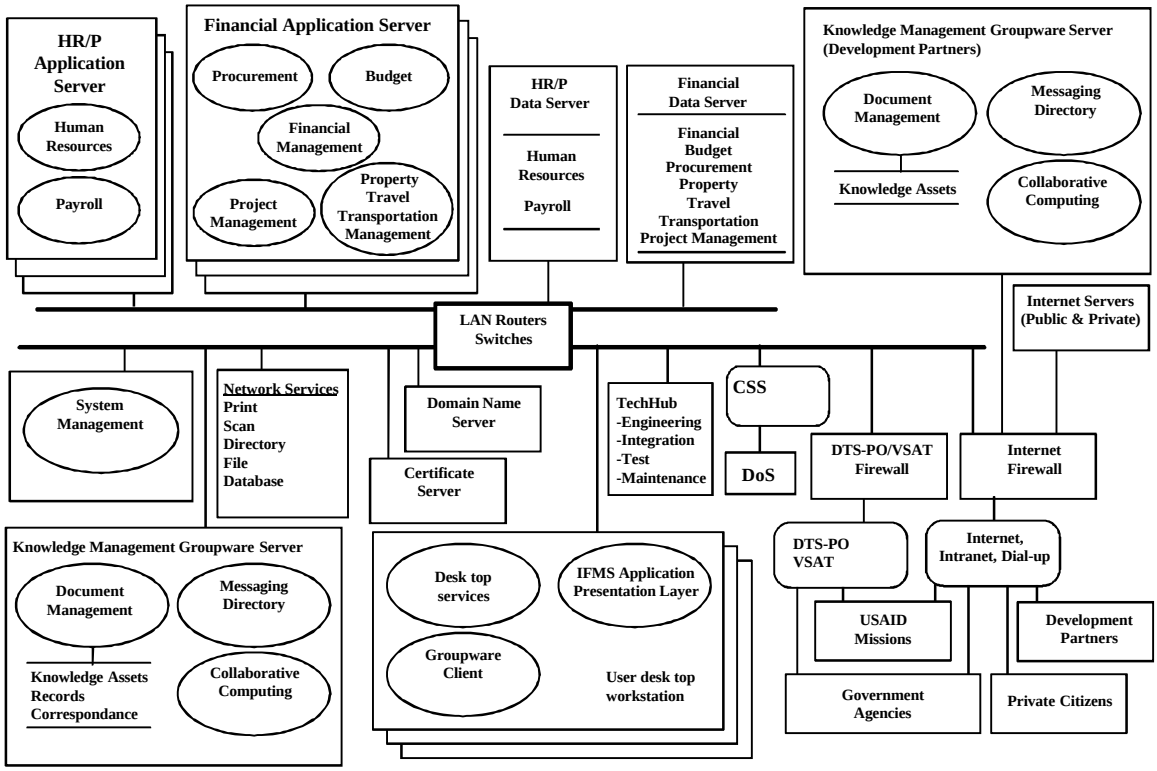



**Figure 9-11. USAID/W Applications (IFMS Option 2), Data, Network Architecture**

## *9.3 Mission Application and Data Architecture*

The USAID missions vary significantly in size (1-300+) and are in locations that have a wide range of long-distance communications infrastructure and technical support. The number and size of missions continues to change in response to world conditions. No single architecture meets the needs of all missions in a manner consistent with available capabilities. Therefore, a range of mission architecture options is required. In the following discussion, IFMS and knowledge management options are discussed together because of their similarity. However, they are not coupled, and one IFMS option can be implemented with a different knowledge management option.

Figure 9-12 depicts the thin client mission architecture option. The user desktop workstation is configured in the mission the same as it is in USAID/W, with desktop services, the groupware client, and the IFMS application presentation layer. Mission users access the applications and data on the central USAID/W servers. Security controls assure that mission users have access to the data they require but are denied access to data that they do not require. This denial can result in the data being read-only or in it being totally inaccessible depending on agency policy.

This option is the standard vendor architecture for IFMS products for a remote site. It is the option that requires the least system administration support in the mission. If it is implemented with no network servers or Internet servers, no local system administration support is required.

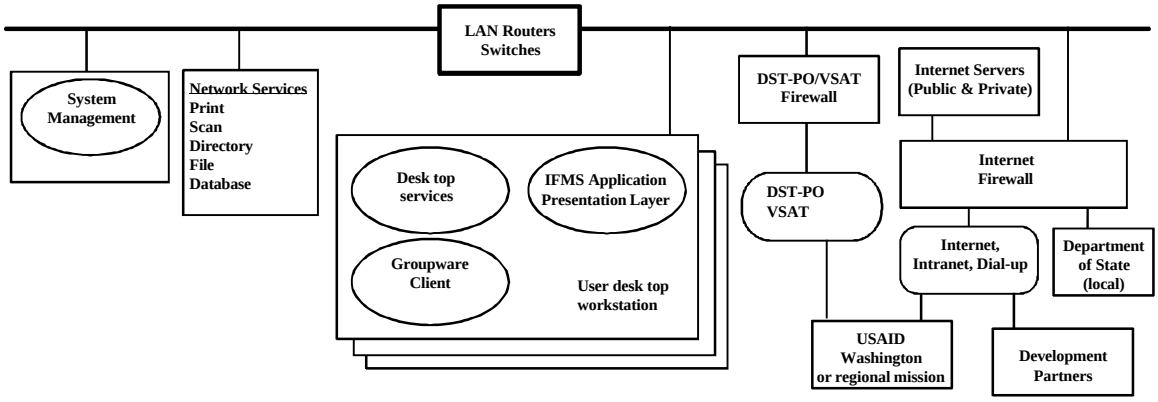



**Figure 9-12. Mission Thin Client Option**

For users to productively work with the system, a mission with one or a few concurrent users requires a link to USAID/W or to a regional support center with a minimum of 64 kbps available bandwidth and less than 1-second latency. Missions with a larger number of concurrent users require additional bandwidth that is dependent on the choice of application vendor and the mix of mission activities. Prototype testing determines performance over the various communications options.

Figure 9-13 depicts the desktop database mission architecture option. The user desktop workstation hosts IFMS applications in a single user mode, groupware software, and data accessed by the user rather than the user accessing data hosted in USAID/W. Table 9-1 lists alternate implementation approaches for the IFMS. This option is only considered for missions too small to support local servers and with inadequate bandwidth for the thin client option. This option can also be implemented with no local system administration support in a small mission.

For groupware products, this is a standard architecture for a remote site. In a limited duration session, the data is replicated between the central knowledge management groupware server and the remote user's desktop workstation where the groupware client accesses it. Security controls assure that mission users have access to the data they require but are denied access to data that they do not require. The replication is selective so that large volumes of data are not transmitted.

Replication works well for email with limited attachments and other low volume databases. Large volume replication requires high bandwidth communications. Missions with limited bandwidth have bulk media (e.g., digital compact disk) delivery of relatively static large databases. They are not able to participate effectively in certain collaborative computing activities.

For IFMS products, this is a nonstandard architecture for a remote site. It is feasible for some products to have a complete software suite on a desktop and a complete database containing only data the mission requires. Missions generally require little or no IFMS data for other missions or USAID/W.

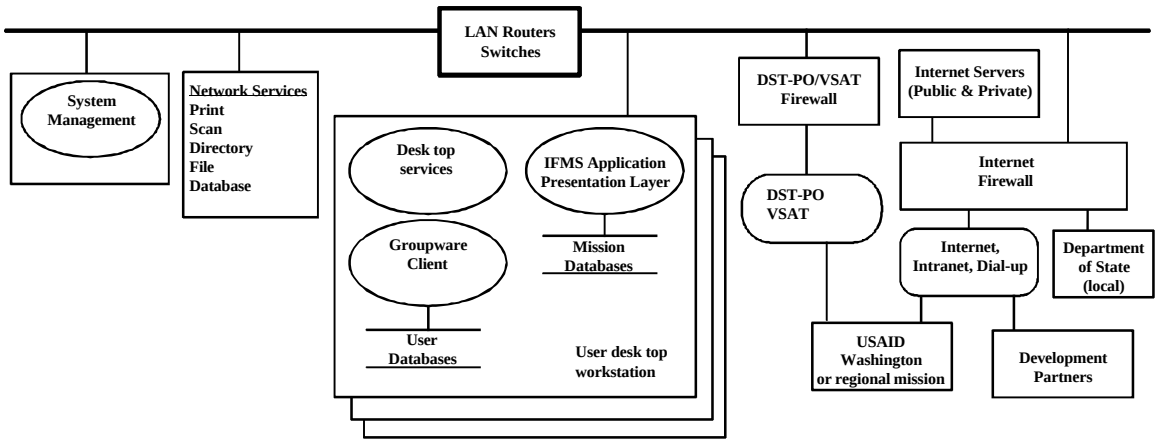



**Figure 9-13. Mission Desktop Database Option**

In a limited duration session, the required mission data is replicated between the central IFMS data server and the remote user's desktop workstation, where the single-user application suite accesses it. Security controls assure that mission users have access to the data they require but are denied access to data that they do not require. The replication is selective so that only the data required by the mission is transmitted. In a similar fashion, USAID/W required mission data (e.g., transactions) are replicated to the central IFMS data server.

The risks for this option are managing the applications and the database replication. The feasibility of a mission with poor communications capability being able to successfully replicate data with USAID/W is questionable and must be determined by prototype testing.

Table 9-1 lists several alternate implementations of this IFMS architecture for the missions that offer possibilities to work around the communications limitations. Rather than replicating the mission's portion of the central database, a subset of the mission's data is extracted into a flat file in a custom format or in a format compatible with the desktop spreadsheet and word processor. The flat files are transferred to the mission periodically or as needed. Users in the missions review and manipulate the data, but their changes are not reflected in the central database. Input from the users in the missions is in forms using a spreadsheet, word processor, or the groupware product forms capability. Periodically or as needed, the forms are transferred as flat files to the USAID/W IFMS applications for final processing to update the central database.

Flat file and forms options are developed and evaluated using a prototype to determine the user's ability to successfully execute mission responsibilities. The options may range from sending a complete copy of all the mission's data to highly summarized reports. The options are tested with various network communications options. For worst case communications situations, physical media transfer is evaluated as well. Because of the opportunity to tailor the data communicated with USAID/W, these implementation options provide significant potential for success.

Figure 9-14 depicts the data server mission architecture option. The mission has a full IFMS application server, an IFMS data server with only the data required by the mission, and a knowledge management groupware server with mission-specific and agency-wide databases. Table 9-1 lists alternate implementation approaches for the IFMS. This option requires resident system administration support.

For groupware products, this is a standard architecture for a remote site. In a limited duration session, the data is replicated between the central groupware server and the remote mission groupware server. Users access the knowledge management data from their desktop workstation using a groupware client. The replication is selective, so that only data needed by the mission are replicated.

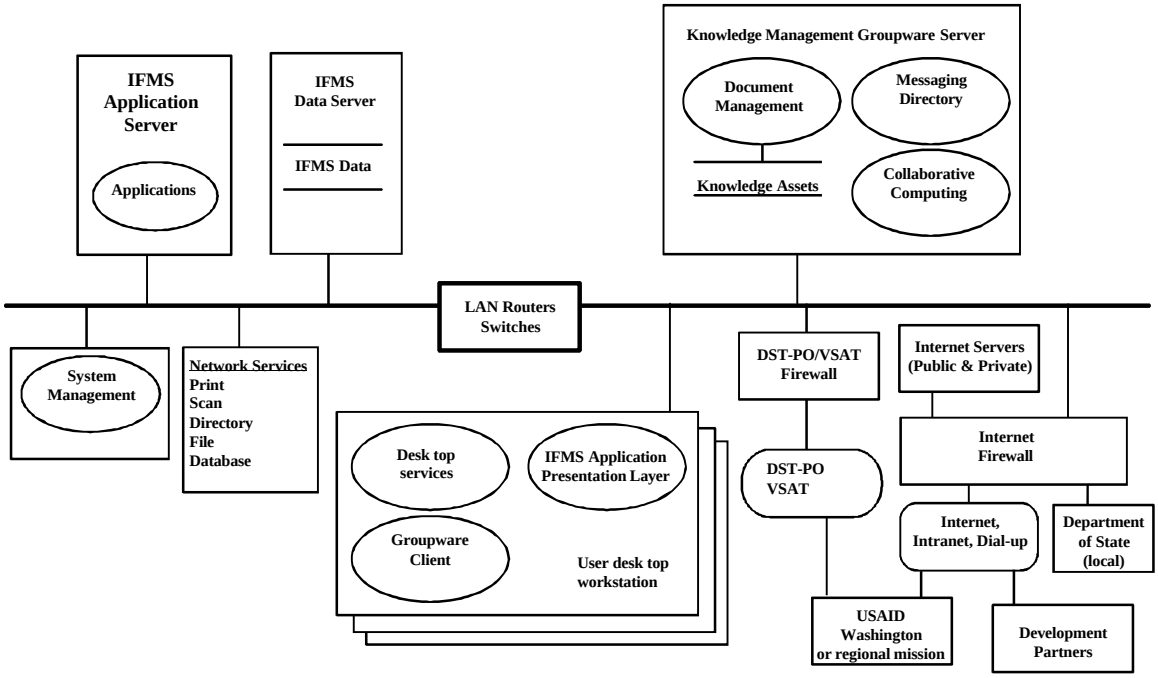



**Figure 9-14. Mission Data Server Option**

For IFMS products, this is a nonstandard architecture for a remote site. The system works the same as in the desktop database option, except users share the application server and the database as they do in USAID/W. The risks for this option are managing the applications and the database replication. The feasibility of a mission with poor

communications capability being able to successfully replicate data with USAID/W is questionable and is determined by prototype testing.

This architecture has the same alternate implementations for the missions as the previous architecture. They both offer possibilities to work around the communications limitations. Rather than replicating the mission's portion of the central database, a subset of the mission's data is extracted into a flat file in a custom format or in a format compatible with the desktop spreadsheet and word processor. The flat files are transferred to the mission periodically or as needed.

Users in the missions review and manipulate the data, but their changes are not reflected in the central database. Input from the users in the missions is in forms using a spreadsheet, word processor, or the groupware product forms capability. Periodically or as needed, the forms are transferred as flat files to the USAID/W IFMS applications for final processing to update the central database. These implementation alternatives do not require a mission application server.

Some of the missions receive significant support from missions operating as regional support centers. The architecture options remain the same for these missions, except that they may communicate data to and from the regional support center rather than USAID/W.

## *9.4 Security Architecture*

The USAID Target Enterprise Information Architecture System Requirements Report specifies the USAID information threat environment and security requirements. Table 9-2 defines and lists the security services and mechanisms required to provide those services. This section discusses the allocation of required security mechanisms to the components of the USAID TEIA depicted in Figure 9-15 for USAID/W and Figure 9-16 for missions. It does not discuss physical, personnel, administrative, or process related security.

USAID systems that contain classified information are not addressed in this architecture. This document addresses only those USAID systems that process, store, or transmit SBU or other unclassified information. Many USAID systems contain multiple categories of SBU information (for example, procurement source evaluation and selection, proprietary, financial, and private personnel data).

A layered approach is used to structure security for the USAID TEIA. Multiple security mechanisms provide overlapping protection. The failure of a single mechanism does not leave USAID's resources completely vulnerable; intruders must still penetrate additional mechanisms.

Many of the mechanisms depend on the use of cryptography. USAID cryptography is based on a public key infrastructure; each user has a private key and a public key. All USAID public keys are distributed via directory services so they are easily available to all users. Data sent to any user over public networks is encrypted with the recipient's public key but can only be decrypted with the recipient's private key. Only the user has access

to his/her private key. Encryption and decryption are performed automatically and require no user action.

**Table 9-2. Required Security Services and Their Implementing Mechanisms**

| Security Service | Security Mechanism |
|---|---|
| **DATA INTEGRITY**: Protects information against unauthorized modification | **Access Control**: A means of restricting access to information. |
| | **Cryptography**: Provides a means (encryption) for rendering information unintelligible and a correlative means (decryption) for restoring encrypted information to intelligible form. |
| | **Error Detection**: To detect errors in transmitted data, some redundant information (e.g., a checksum) is included with the transmission, and this enables the receiver to determine that an error has occurred. |
| **PROTECTION AGAINST DENIAL OF SERVICE** (sometimes called "Availability"): Protects against unauthorized withholding of information and resources from authorized users. | **Data Replication**: The duplication of data at multiple storage locations. |
| | **Adaptive Routing Algorithms** (a.k.a. dynamic routing): Algorithms that change their decisions regarding the routing of packets based upon changes in network topology and traffic. |
| **DATA CONFIDENTIALITY**: Protects information against unauthorized disclosure | **Access Control** (see definition above) |
| | **Cryptography** (see definition above) |
| **ACCOUNTABILITY**: Enables security-relevant activities on a system to be traced to those persons who perform them | **Identification and Authentication (I&A)**: In the I&A process (a.k.a. "login"), a user identifies herself (e.g., with a userid) and offers proof of the identity (e.g., with a password). |
| | **Audit**: An audit mechanism provides a means to record information regarding the security-relevant actions of system users. It also provides means for a privileged administrator to review that audit information. |
| | **Digital Signature**: Provides legal proof of the originator's identity and confirmation that the message sent is exactly the same as the message received. Can also provide proof that a message was received unmodified by the intended addressee. |

| Security Service | Security Mechanism |
|---|---|
| **SECURITY MANAGEMENT**: Enables security and system administrators alone to initialize and maintain security services and mechanisms | **Protected Security Administrator Interface**: An interface by which privileged users manage security mechanisms. |
| | **Intrusion Detection**: Detects the actions of persons attempting to gain unauthorized access to an information system and reports them to security managers—sometime in real time. |
| | **Malicious Code Detection**: Detects the presence of viruses, Trojan horses, worms, trapdoors, logic bombs, and other types of malicious code. |
| | **Vulnerability Detection**: Checks the configuration of OSs and network services for vulnerabilities. |

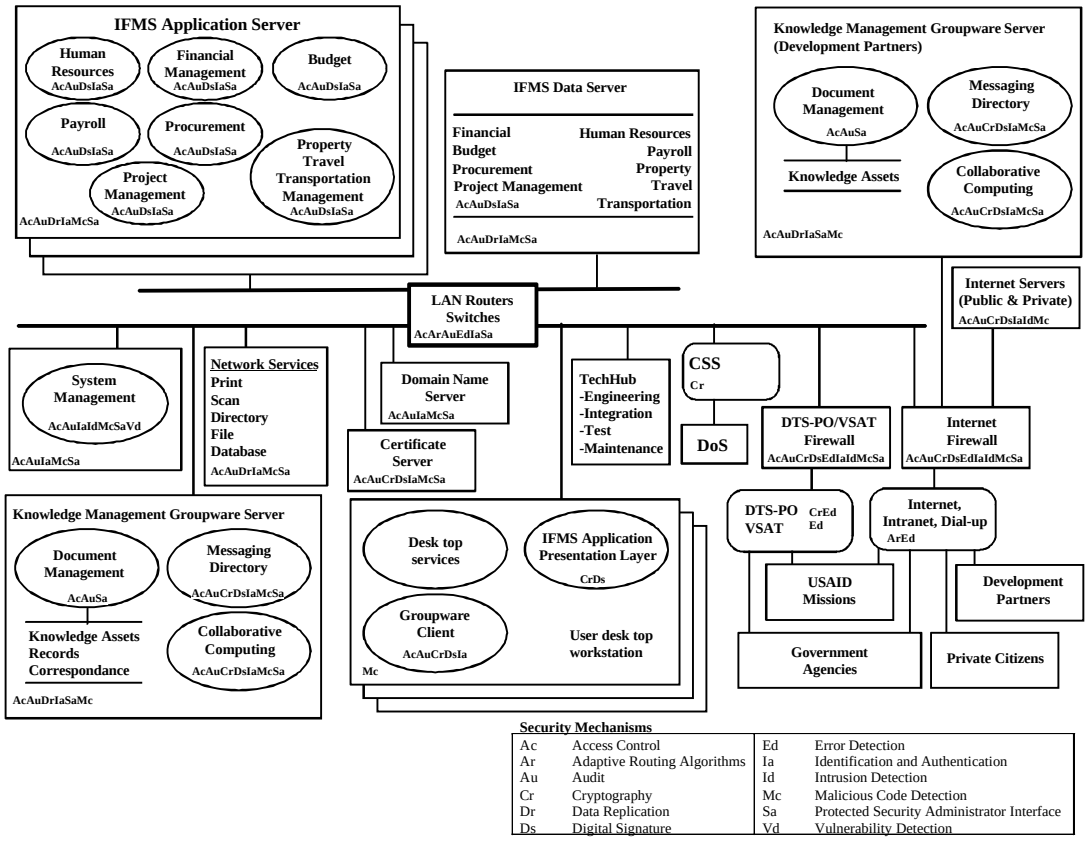



**Figure 9-15. USAID/W Security Architecture**

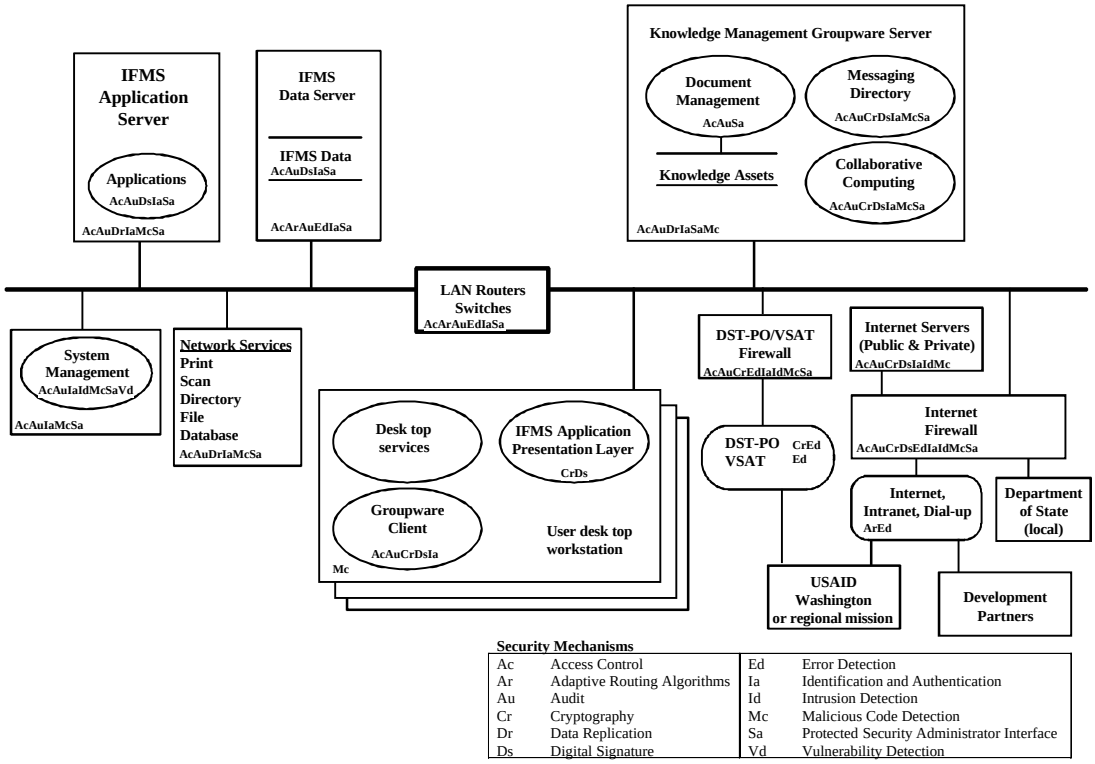



**Figure 9-16. Mission Security Architecture**

### 9.4.1 Network Security Mechanisms

Firewalls implement the outer layer of protection of USAID's information assets. Firewalls implement digital signatures to provide strong identification and authentication of users requesting access via WANs or dial-up remote access systems (RASs). Access control, intrusion detection, and malicious code detection mechanisms in the firewalls assure that only authenticated users have access to network assets. Security administrators control the firewall by using the security management capabilities of the system management software.

Cryptography also assures the confidentiality and integrity of data traversing the WAN. Firewalls, routers, and switches provide error detection to support the integrity of the data. Adaptive routing in network routers supports the availability of the data. Switches and routers protect the LAN with access control, identification and authentication, audit, and protected security administrator interface mechanisms.

### 9.4.2 Server Workstation Security Mechanisms

Server workstations provide the next layer of security mechanisms through their OS and security products. (Section 9.4.4 discusses application and data security mechanisms.) Only system administrators are permitted to execute system administration functions.

Users attempting to access servers are identified and authenticated to control access to server assets. Access to security controls is via a protected security administrator interface. Because internal users are trusted not to sniff network messages or attempt to subvert security mechanisms, cryptography is not required to protect LAN communications. However, all server actions are recorded in an audit file for incident investigation.

System management applications centrally administer user accounts, user access control, and firewalls through their security management capabilities. They provide two additional security mechanisms not provided by other applications. Vulnerability detection software assesses the state of server OSs looking for known system configuration vulnerabilities. Intrusion detection software looks for suspicious or unusual activity indicating an intruder on the network, servers, and client workstations. They integrate audits collected by network devices for analysis, reporting, and action.

Malicious code detection software on all servers examines files for computer viruses and other malicious code intended to disrupt normal server functioning. Data replication software on network file and data servers protects their availability in the event of hardware failure or data corruption.

### 9.4.3 Client Workstation Security Mechanisms Client

Client workstations are configured so that they cannot be accessed from the network except by system administration functions. (Section 9.4.4 discusses application and data security mechanisms.) Data on the workstations are protected by physical access control. Workers who share physical space are trusted to not access another worker's data on their workstation without permission. The only security mechanism enabled on the client workstations is malicious code detection. Malicious code detection software examines files for computer viruses and other malicious code intended to disrupt normal workstation functioning.

### 9.4.4 Application Software and Data Security Mechanisms

Application software and data base management systems provide an additional layer of protection. The application software in the TEIA is expected to be predominantly COTS. The security architecture reflects the security mechanisms generally provided by vendors for each class of software. If the selected products do not provide these mechanisms, the security architecture will have to be modified to meet the security requirements.

In the three-tier IFMS architecture described in Section 0, the applications control the access to the database. Therefore, vendors have implemented strong identification and authentication, access control, audit, and protected security administrator interfaces in the application software. Digital signature mechanisms in the application presentation layer and application software strengthen the assurance level for authentication of users granted access to highly sensitive data. Database administrators and certain users are authorized to query the database directly. Strong identification and authentication, access

control, audit, and protected security administrator interface mechanisms in the database management system (DBMS) software protect the data.

Knowledge management groupware products provide similar mechanisms. In addition, because they are designed to share non-real-time data messages over potentially unprotected WANs, these products also provide built-in cryptography and digital signature in both client and server components to protect data in transit and stored on servers. They also scan message attachments for malicious code signatures and prohibit transmission of messages containing these signatures.

Most desktop applications (e.g., spreadsheets and word processors) do not require security mechanisms because they are intended for local use only. (Some have implemented malicious code detection.) Internet applications such as browsers are the exception because they are intended to share data over potentially unprotected WANs. Therefore, vendors provide built-in cryptography and digital signature mechanisms to protect data in transit.

## *9.5 External Interfaces*

In performing its mission, USAID interacts with several external entities by exchanging documents, reports, data, and information. External entities are both U.S. Government and non-U.S. Government entities. Information exchanged with other Government entities is required to meet USAID's legal responsibilities. Information exchange with entities belonging to private or public sectors, either national or foreign, is primarily to facilitate or execute the agency's mission.

The U.S. Government external interface entities include:

- U.S. Congress
- Office of Management and Budget
- U.S. Department of State
- U.S. Department of Treasury
- U.S. Department of Health and Human Services
- Other U.S. agencies and administrations such as General Services Administration, Small Business Administration, and National Institutes of Health
- USAID employees, either civil service (CS), foreign service (FS), or foreign service national (FSN), interacting with the agency as individuals or within their roles

USAID employees are included as external interface entities because they are external to the information systems. All information system architectures must recognize their respective users as external interfaces to assure that their needs are met. They are, in fact, the most important external entities because the majority of system capabilities are implemented to meet their needs. This does not imply that the employees are external to the agency.

The non-U.S. Government external interface entities include the following:

- Customers, the individuals or organizations benefiting from or affected by USAID services or products
- Partners, the external organizations with whom USAID cooperatively defines objectives and carries out programs to achieve them (including PVOs, NGOs, universities, businesses, and other international assistance organizations)
- Host country governments that develop with USAID missions strategic objective agreements providing the context for the interactions with customers and partners (host country governments may also have partner roles)
- United States or foreign financial institutions
- Vendors, the providers of products or services (who may also have partner roles)

Each USAID business area interacts with a subset of the USAID external entities (see Appendix E.) Program operations interacts mainly with customers, host country governments, and partners. Budget interacts with the U.S. Congress, the OMB, and the U.S. Department of State. A&A interacts with vendors, NIH, OMB, Budget, the U.S. Congress, and the Small Business Administration (SBA). Human resources interacts mainly with employees. Financial management interacts primarily with the U.S. Treasury, the U.S. Department of State, United States and foreign financial institutions, partners, and vendors. Property management interacts with vendors and employees. Knowledge management interacts primarily with partners and other U.S. agencies and administrations.

# 10. Conclusion

This report describes the target Enterprise Information Architecture for USAID. The components include the application, data, technical, and security architectures. The process architecture is in the system requirements report. This report addresses USAID's Washington, D.C., location and its foreign mission locations. It includes three operations concepts and mission architectures that enable missions of all sizes and technical capabilities to function successfully.

The architecture provides the information systems necessary for USAID to meet its financial management requirements. USAID must implement detailed controls, processes, and procedures consistent with required management practices. In addition, USAID must implement an accounting cost structure to capture financial data at a level of detail and organization that will enable effective management and reporting of the agency's resources. The combination of management practices, accounting cost structure, and information systems enables USAID to be compliant with all related Government laws and regulations.

The knowledge management components of the TEIA provide a platform for initiating a new era of improved information sharing to support all authorized users in planning, implementing, and evaluating the agency's business. Knowledge management and virtual

work environments offer enormous potential for improvement in the quality and productivity of the business processes they support. However, experience with these environments is limited, and each organization's needs are different.

Use of the capabilities presented here provides a basis for USAID to more clearly understand how to leverage knowledge management and identify additional capabilities for expanded value to the agency. The specific components were chosen to assure the highest probability that an immediate benefit would be accrued at limited cost with minimal implementation risk. As USAID gains experience with knowledge management and as the technology evolves, new capabilities will be added.

The security architecture enables USAID to operate its global organization effectively while protecting valuable information in a manner compliant with the *Computer Security Act*. Along with WAN technology, the security architecture is the enabling technology for assuring all authorized users secure access to planning, implementation, and evaluation data.

The flexible mission architecture supports the dynamic changes in mission staffing and location. Improved efficiency from COTS products increases the efficiency of the remaining members of USAID's declining Washington staff. The COTS products provide improved functionality and performance while reducing operations and maintenance cost.

The transition from the Y2K baseline to the target architecture is made in a sequence of steps. Each step results in an intermediate state that supports USAID operations with improved capability and performance at lower cost. The steps in the IFMS transition are being planned and documented in the *IFMS Modernization Plan*.

The office of the Chief Financial Officer (CFO) is selecting the core financial management product. At completion of these efforts, the IFMS architecture is chosen on the basis of the product selected, and an Enterprise Information Architecture transition plan is developed to specify and plan these states. The schedule for the transition plan will be constrained by available funding.

At the completion of each step in the transition plan, USAID information systems approach the following vision:

> USAID information management systems provide every employee access to the tools and information at his/her workstation necessary to carry out the agency's mission with the highest level of responsible stewardship of federal resources. The systems promote information sharing and collaboration with USAID international development partners to achieve shared strategic objectives (SOs).

## 11. Abbreviations and Acronyms

| | |
|---|---|
| A&A | Acquisition and Assistance |
| AETA | American Electronic Time and Attendance (System) |
| AFR | Africa (Bureau) |
| AIX | Advanced Interactive Executive (IBM) |
| ANE | Asia Near East (Bureau) |
| BHR | Bureau for Humanitarian Response |
| BUD | Budget |
| CFO | Chief Financial Officer |
| CN | Congressional Notification |
| CO | Contracting Officer |
| COBRA | Consolidated Omnibus Reconciliation Act |
| COTS | commercial off-the-shelf |
| CP | Congressional Presentation |
| CS | Civil Service |
| CSS | Cable Switching System |
| DBMS | database management system |
| DCIA | Debt Collection Improvement Act |
| DHHS | Department of Health and Human Services |
| DTS-PO | Diplomatic Telecommunications Services–Program Office |
| ECS | Electronic Cable System |
| EDI | Electronic Data Interchange |
| EDIPAC | Electronic Data Interchange Payment and Collection |
| E&E | Europe and Eurasia (Bureau) |
| EOP | Equal Opportunity Program |
| FDDI | fiber-optic distributed data interface |
| FM | Financial Management |
| FMFIA | Federal Managers Financial Integrity Act |
| FNS | FDDI Network Services |
| FS | Foreign Service |

| | |
|---|---|
| FSN | Foreign Service National |
| GAO | Government Accounting Office |
| GC | General Counsel |
| GOALS | Global Online Accounting Link System |
| GPRA | Government Performance and Results Act |
| GSA | General Services Administration |
| GUI | graphical user interface |
| HR | Human Resources |
| IAHB | Interagency Housing Board |
| IFMS | integrated financial management system |
| IP | Internet protocol |
| ITA | International Trade Association |
| ITMRA | Information Technology Management Reform Act |
| JFMIP | Joint Financial Management Improvement Program |
| LAC | Latin America and the Caribbean (Bureau) |
| LAN | local area network |
| LOC | Letter of Credit |
| LPA | Bureau for Legislative and Public Affairs |
| MACS | Mission Accounting and Control System |
| NAPS | New American Payroll System |
| NFC | National Finance Center |
| NGO | non-governmental organization |
| NIH | National Institutes of Health |
| NMS | New Management System |
| NOS | Network Operating System |
| OMB | Office of Management and Budget |
| OPAC | Online Payment and Collection |
| OPM | Office of Personnel Management |
| OPS | Operations |
| OYB | Operating Year Budget |
| PAID | Payment Advice Internet Deliver |

| | |
|---|---|
| PM | Program Management |
| PPC | Policy and Program Coordination (Bureau) |
| PRIME | Principal Resource for Information Management Enterprisewide |
| PSC | personal services contractor |
| PTA | Paying and Transfer Agent |
| PVO | private voluntary organization |
| RAMPS | Revised Automated Manpower & Personnel System |
| RAS | Remote Access System |
| RITS | Retirement and Insurance Transfer System |
| RPMS | Real Property Management System |
| RRB | Ronald Reagan Building |
| SA | System Architect |
| SBA | Small Business Administration |
| SBU | sensitive but unclassified |
| SDBU | Small and Disadvantaged Businesses Utilization |
| SDLC | synchronous data link control |
| SO | Strategic Objective |
| SSA | Social Security Administration |
| TCP | transmission control protocol |
| TEIA | target Enterprise Information Architecture |
| TN | Technical Notification |
| TOPS | Treasury Offset Program System |
| TROR | Treasury Report on Receivables |
| USDO | United States Disbursing Office |
| USG | U.S. Government |
| UNICEF | United Nations Children's Fund |
| USAID | United States Agency for International Development |
| USAID/W | USAID, Washington |
| USDA | U.S. Department of Agriculture |
| VLAN | Virtual LAN |

| | |
|---|---|
| VSAT | very small aperture terminal |
| WAN | wide area network |
| WHO | World Health Organization |

## 12. References

*Accounting and Auditing Act of 1950*

*Chief Financial Officers Act of 1990*

*Computer Security Act*

*Federal Managers Financial Integrity Act of 1982 (FMFIA)*

*Government Performance and Results Act (GPRA) of 1993* (Public Law 103-62)

*Information Technology Management Reform Act (ITMRA) of 1996* (40 USC 1401 et seg.)

*Inspector General's Audit of the Extent to Which USAID's Financial Management System Meets Requirements Identified in the Federal Financial Management Improvement Act of 1996* (Audit Report No. A-000-98-003-P), March 2, 1998

OMB Circular No. A-11, October 25, 1996

OMB Circular No. A-127, Subject: Financial Management Systems, July 23, 1993

OMB Budget Bulletin No. 93-02

OMB Circular No. A-125, 31 USC Section 3901, *Prompt Payment Act*

*Review of Material Weaknesses Reported in FY 1998 Federal Managers Financial Integrity Act*

*Reform Roadmap 1999-2000, Annex A, Agency-Wide Systems*

*USAID Strategic Plan*, September 1997

*USAID Y2K Baseline Architecture Report, Revision 1,* October 1999

*USAID Target Enterprise Information Architecture System Requirements Report*, February 2000

# Appendix A. Federal Enterprise Architecture Conceptual Framework

The CIO Council's Federal Enterprise Architecture Conceptual Framework consists of eight components:

1. Architecture drivers, represents an external stimulus which causes the enterprise architecture to change

2. Strategic direction guides the development of the target Architecture, and consists of

    - Vision which is a statement defining the targeted end state for the architecture in five years
    - Goals & objectives for reaching the vision
    - Principles for guiding the architecture development

3. The current technology architecture consists of three technology sub-architectures:

    - Current data architecture, which consists of data models
    - Current system architecture, which consists of system models
    - Current infrastructure architecture, which consists of infrastructure models

4. The target technology architecture consists of three technology sub-architectures:

    - Target data architecture, which consists of data models
    - Target system architecture, which consists of system models
    - Target infrastructure architecture, which consists of infrastructure models

5. The technology models consist of three types of models:

    - Data models, which are used for defining the current and target data architectures
    - System models, which are used for defining the current and target system architectures
    - Infrastructure models, which are used for defining the current and target infrastructure architectures

6. The technology architecture segments consist of three technology sub-architectures:

    - Data architecture segments, which consist of data models
    - System architecture segments, which consist of system models
    - Infrastructure architecture segments, which consist of infrastructure models

7. Transitional processes consist of any processes that support the migration from the current architecture to the target architecture. Examples include the following:

    - Investment review, which involves providing architecture information to support the investment review decision process

- Segment coordination, which entails coordinating the integration of the segment architectures into the enterprise architecture
- Market research, which is a periodic market scan to identify new technologies with potential benefits
- Asset management, which entails managing all Federal architecture assets

8. Standards refer to all mandatory standards, guidelines, and best practices, and also include profiles that are configuration options for implementing the standards. Examples include:

    - Security standards, which apply to all levels of security
    - System standards, which apply to application systems
    - Data standards, and apply to data
    - Infrastructure standards, which apply to the infrastructure

Section 4 and Section 6 discuss the architecture drivers.

Section 2 and Section 7 discuss the strategic direction.

The current technology architecture is discussed in Section 5 and documented in the *USAID Y2K Baseline Architecture Report.*

Section 9 discusses the target technology architecture, technology models, and technology architecture segments. Data and systems models appear in Section 9.1 for USAID/W and Section 9.3 for the missions. Section 9.5 provides details on the data model for external interfaces. Infrastructure models are in Sections 9.2 and 9.3. Business process models are discussed in Section 3 and documented in the *USAID Target Enterprise Information Architecture System Requirements Report.*

Transitional processes are documented elsewhere.

A standards model for USAID will be provided in the *USAID Target Enterprise Information Architecture System Design Report.*

## Appendix B. Raines' Rules

The following is an excerpt from an October 25, 1996, Office of Management and Budget memorandum.

SUBJECT: Funding Information Systems Investments

The *Information Technology Management Reform Act* (ITMRA) of 1995 (40 USC 1401 et seg.) directs the Office of Management and Budget to establish clear and concise direction regarding investments in major information systems, and to enforce that direction through the budget process. Accordingly, the decision criteria set out below are established with respect to the evaluation of major information system investments proposed for funding in the FY 1998 President's budget.

The most effective long-term investment strategy is guided by a multiyear plan. The plan is a roadmap for getting from "where we are today to "where we want to be" – achieving the strategic mission goals of the organization in the framework of the *Government Performance and Results Act* (GPRA). Thus, the first four decision criteria relate specifically to capital planning. The fifth criterion establishes the critical link between planning and implementation – information architecture – which aligns technology with mission goals. Under the ITMRA, the Chief Information Officer is responsible for that architecture. The last three criteria establish risk management principles to assure a high level of confidence that the proposed investment will succeed.

Policy

Investments in major information systems proposed for funding in the President 's budget should:

1. support core/priority mission functions that need to be performed by the Federal government;

2. be undertaken by the requesting agency because no alternative private sector or governmental source can efficiently support the function;

3. support work processes that have been simplified or otherwise redesigned to reduce costs, improve effectiveness, and make maximum use of commercial, off-the-shelf technology;

4. demonstrate a projected return on the investment that is clearly equal to or better than alternative uses of available public resources. Return may include: improved mission performance in accordance with GPRA measures; reduced cost; increased quality, speed, or flexibility; and increased customer and employee satisfaction. Return should be adjusted for such risk factors as the project's technical complexity, the agency's management capacity, the likelihood of cost overruns, and the consequences of under- or non-performance

5. be consistent with Federal, agency, and bureau information architectures which: integrate agency work processes and information flows with technology to achieve the agency's strategic goals; reflect the agency's technology vision and year 2000 compliance plan; and specify standards that enable information exchange and resource sharing, while retaining flexibility in the choice of suppliers and in the design of local work processes;

6. reduce risk by: avoiding or isolating custom-designed components to minimize the potential adverse consequences on the overall project; using fully tested pilots, simulations, or prototype implementations before going to production; establishing clear measures and accountability for project progress; and, securing substantial involvement and buy-in throughout the project from the program officials who will use the system;

7. be implemented in phased, successive chunks as narrow in scope and brief in duration as practicable, each of which solves a specific part of an overall mission problem and delivers a measurable net benefit independent of future chunks; and,

8. employ an acquisition strategy that appropriately allocates risk between government and contractor, effectively uses competition, ties contract payments to accomplishments, and takes maximum advantage of commercial technology.

# Appendix C. Example Process Scenarios

This section presents example scenarios that reflect the roles of individuals in executing a portion of an agency business process. They are not the only possible scenarios, as the roles and job assignments could be different, and the order of actions could change. These scenarios are intended to highlight both the similarities and differences associated with process execution given the different mission operations concepts.

The scenarios are depicted as event trace diagrams. Figure C-1 summarizes the components of an event trace diagram. Each individual role is depicted as a vertical bar, with an identifier at the top of the bar. Information transfers are indicated as named horizontal arrows originating at the source and pointing to the recipient. The function or action taken in response to the information transfer is not specified in the diagram and must either be inferred or identified in the process flow diagrams in the *System Requirements Report*.

The information transfers are placed in time order, with the earliest at the top of the bars and later transfers appearing farther down on the page. The two-headed named arrow represents one or a series of two-way communications that could be by phone, e-mail, fax, or any other mechanism. The IFMS automatically generates alerts to notify an individual to execute a step in the scenario. Alerts are generally not depicted in the diagram to improve readability. Alerts are illustrated in one example diagram as dashed arrows.

## *C.1 Acquisition Scenarios*

Figure C-2 depicts an acquisition scenario using the centralized operations concept. Figure C-3 shows the identical scenario with all alerts indicated by dashed arrows. Because all users access the centralized system, there is no change in the scenario whether the individual is located in a mission, a regional support center, or USAID/W. The scenario presumes that an A&A fiscal year plan (FY plan) has been developed and is available in the central agency database.

The requester, in this case a member of a strategic objective (SO) team, reviews the A&A FY plan to assure that funds have been planned for this specific acquisition. The requester uses a desktop tool such as an electronic form to create the request. The request is submitted electronically to the agency database via the IFMS application software, which is not shown in the scenario diagrams.

The negotiator is alerted that a request has been submitted. (Alternatively, the contracting officer may receive the alert and assign the request to a negotiator.) The negotiator reviews the request and identifies potential vendors. He/she negotiates revisions to the request with the requestor. When all aspects of the request are completed to the mutual satisfaction of the negotiator and requester, the negotiator approves the request, and the system alerts the requester, contracting officer, and the SO team leader.

The SO team leader reviews the request within the context of the A&A FY plan, approves the request, and commits funds to the acquisition. The approval and funds commitment are automatically recorded in the agency database. Alternatively, the SO team leader can reject the request and terminate the process or can require further revisions to the request.

The negotiator and the requester are alerted to the SO team leaders' approval and funds commitment. Other individuals, such as the executive officer or mission director, may also receive these alerts. The negotiator reviews the funds commitment, issues a solicitation to the vendor community, and records the solicitation in the agency database. Solicitation responses are evaluated by the negotiator and, if required, by an independent evaluation panel.

The contracting officer selects the winner on the basis of the evaluations. The contracting officer obligates the funds, enters the award in the agency database, and notifies the vendors. The IFMS alerts the requester, team leader, and negotiator that the selection has been made.

Figure C-4 depicts the same scenario modified for the hybrid concept with the contracting officer and negotiator in USAID/W and the SO team at the mission. All steps performed by individuals in the scenario remain the same. Each mission action must be transmitted to USAID/W, where it is recorded in the permanent records of the agency. Each USAID/W action is directly recorded in the agency database and transmitted to the mission. The mechanism and format used to transmit data between the mission files and the agency database is to be determined in the design process.

Figure C-5 is the same as Figure C-4 except that the contracting officer and negotiator have moved out to the mission. The change is that the contracting officer and negotiator execute their transactions using tools in the mission. Communication among process participants in the mission is via a workflow management tool rather than through central database mechanisms. Data files reflecting these actions are transmitted from the mission to USAID/W, where they are automatically entered in the agency database.

The scenario for the distributed concept would look identical to either Figure C-4 or Figure C-5. The key differences are the underlying tools for executing the mission portion of the process, the mechanism for copying information to the agency database, and the fact that mission staff would have access to the full mission portion of the agency database rather than reports transmitted from USAID/W.

## *C.2 Property Management Scenarios*

Figure C-6 depicts a property management scenario using the centralized operations concept. Because all users access the centralized system, there is no change in the scenario whether the individual is located in a mission, a regional support center, or USAID/W. The scenario presumes that a capital asset acquisition award has been issued to a vendor as the result of an acquisition process.

The vendor receives the award and ships the new property to the property manager. The property manager role may be performed by a specialist in some large locations or may be assigned to one or several individuals as a secondary function in smaller locations. The property manager inspects the property to determine if it conforms to acceptance criteria that are part of the acquisition specifications and stored in the agency database. Assuming the property conforms to the criteria, the property manager applies a barcode to the property and records the item in the agency database. The property manager then issues the property to the requester, records the issuance of the property, and executes a notification of receipt for the negotiator (not shown in the figure), contract officer, and any other concerned individual.

In addition to the property, the vendor sends an invoice to the controller. The invoice may be sent at the same time as the property. The controller records the invoice in the agency database, and the property manager is alerted. The property manager reviews the invoice and, on the basis of the property inspection, authorizes payment for the property. The agency database alerts the controller that payment has been authorized, and the controller issues a payment action.

As part of the property management process for new capital assets, the property manager enters into the agency database an initial asset value and the capitalized asset depreciation for the property. This enables the agency to account for the value of the property in its annual financial report.

Figure C-7 depicts the same scenario for the hybrid operations concept with the controller in USAID/W. All steps performed by individuals in the scenario remain the same. Each mission action must be transmitted to USAID/W, where it is recorded in the permanent records of the agency. Each USAID/W action is directly recorded in the agency database and transmitted to the mission. The mechanism and format used to transmit data between the mission files and the agency database is to be determined in the design process.

Figure C-8 depicts the same scenario for the hybrid operations concept with the controller in the mission. The controller enters the invoice in the mission data files. This entry consists of completing an electronic entry, the form of which depends on the design. Using a workflow tool, the system sends the invoice directly to the property manager when the controller completes the data entry. Because in the hybrid concept the mission does not maintain a complete database, the invoice entry must be sent to USAID/W for entry in the agency database ,where it is linked to the other records for this property. The same steps apply to the notification of receipt and the payment authorization.

The scenario for the distributed concept would look identical to either Figure C-7 or Figure C-8. The key differences are the underlying tools for executing the mission portion of the process, the mechanism for copying information to the agency database, and the fact that mission staff would have access to the full mission portion of the agency database rather than reports transmitted from USAID/W.

## *C.3 Summary*

The scenarios depicted in this appendix are examples chosen to illustrate how the system is used to execute business processes. Detailed scenarios will be worked out for each process as the elements of the system are designed, implemented, and deployed. The order of events and assignment of roles may differ somewhat from the depiction in this appendix.

As illustrated in these scenarios, the individual roles are not dependent on the operations concept selected or on the location of the individuals. The tools and the mechanisms for sharing information between the mission and USAID/W are significantly different and bring different benefits, risks, and costs to the agency.

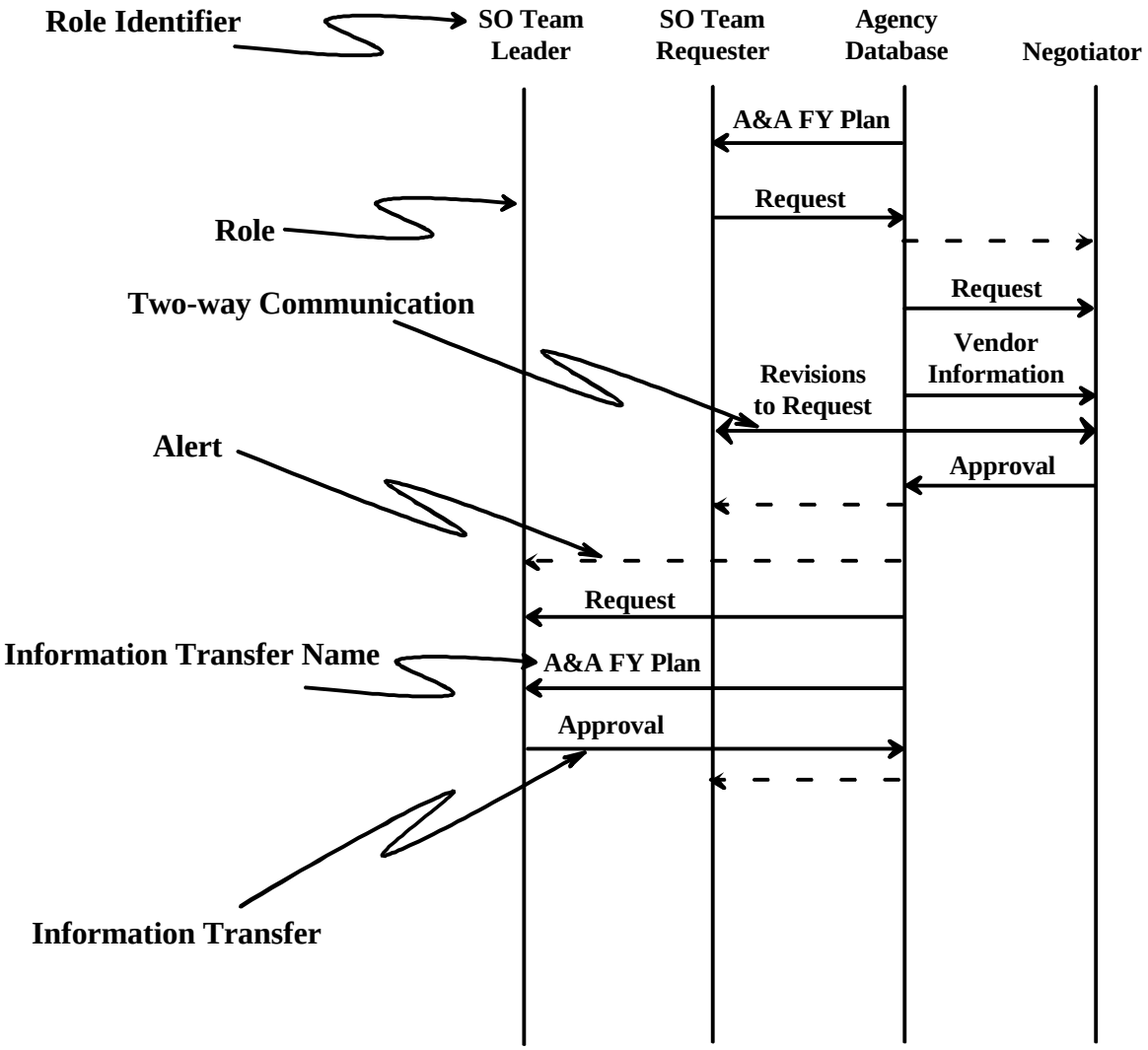



**Figure C-1. Event Trace Diagram Legend**

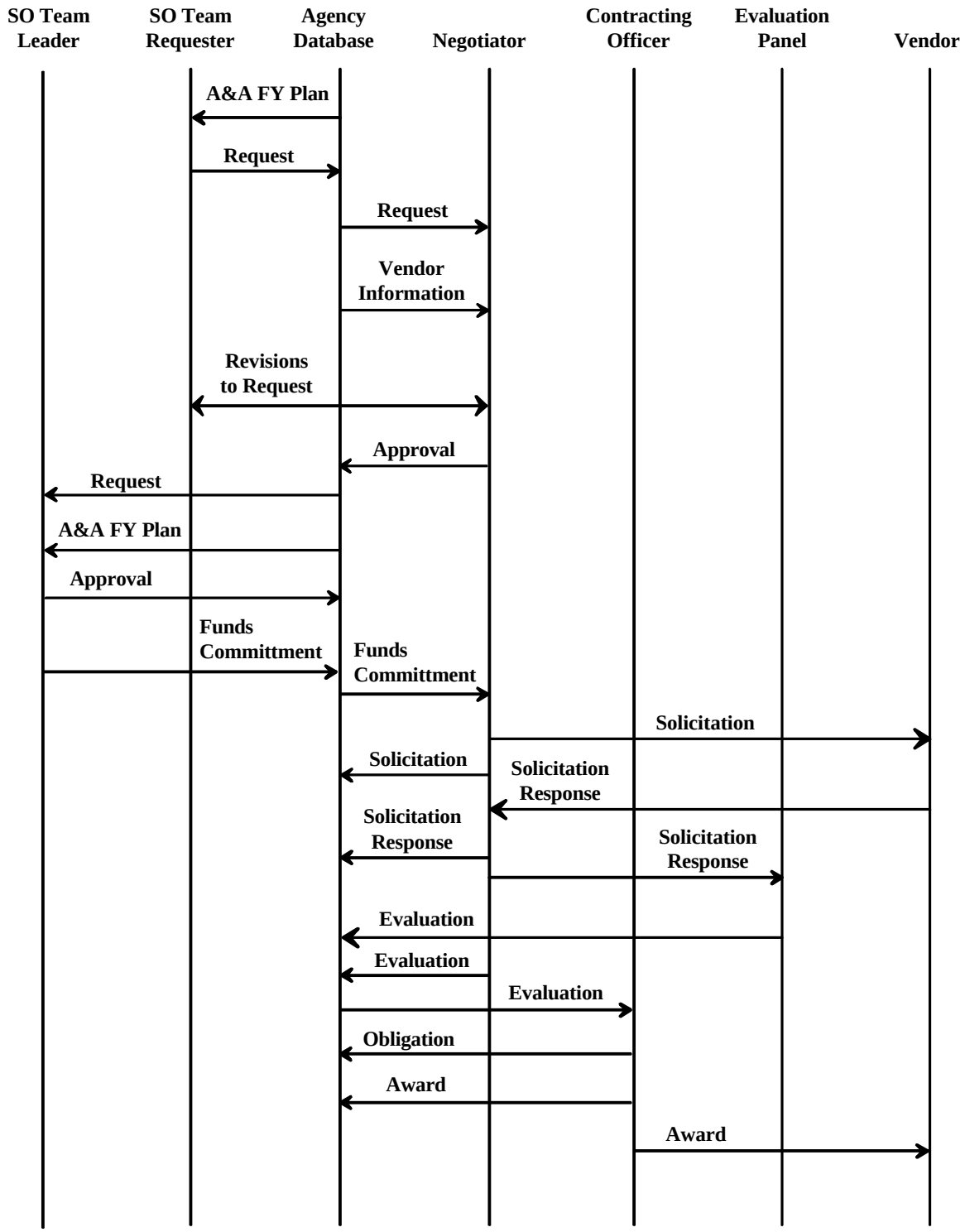



**Figure C-2. Acquisition Scenario for Centralized Operations Concept**

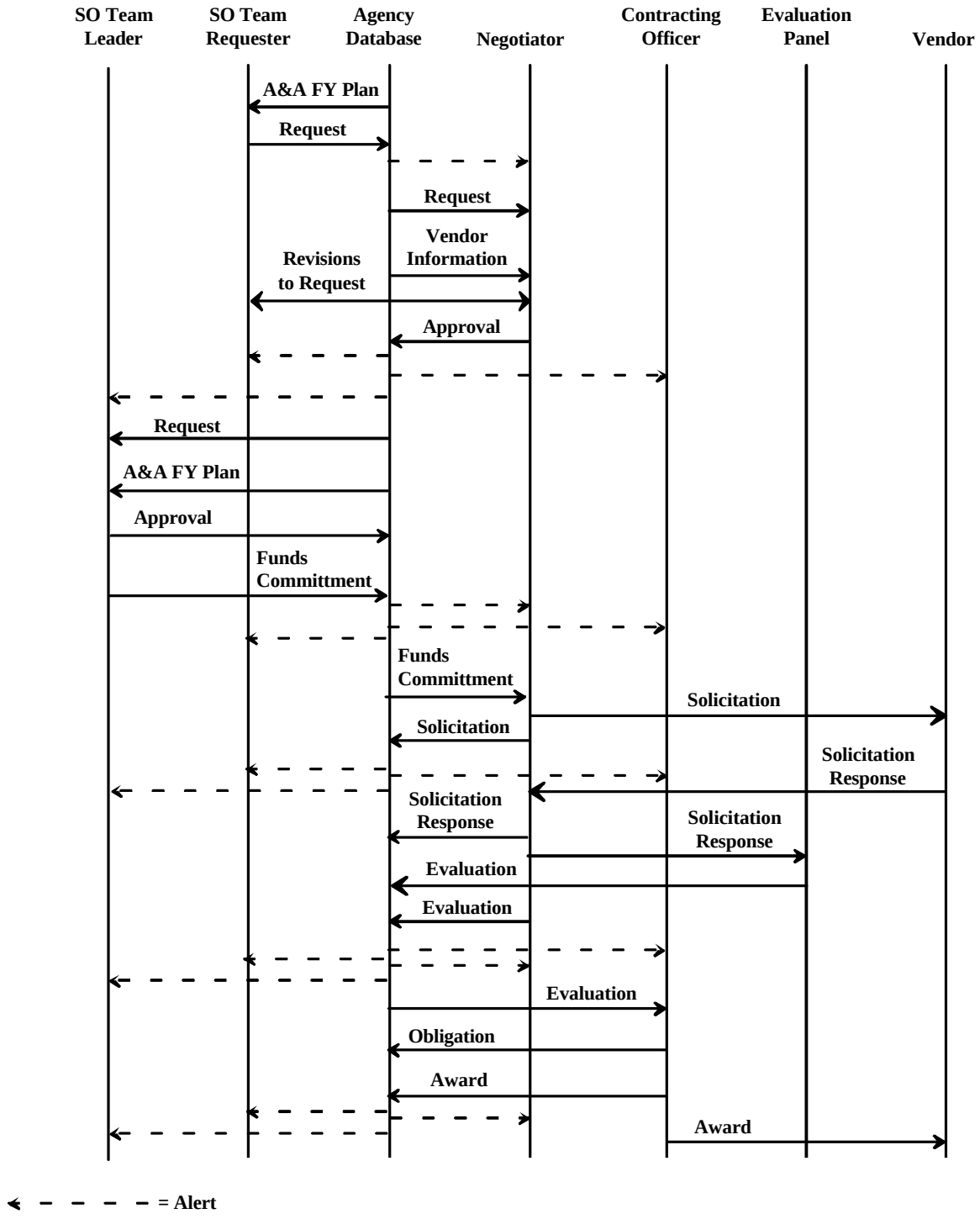



**Figure C-3. Acquisition Scenario With Alerts for Centralized Operations Concept**

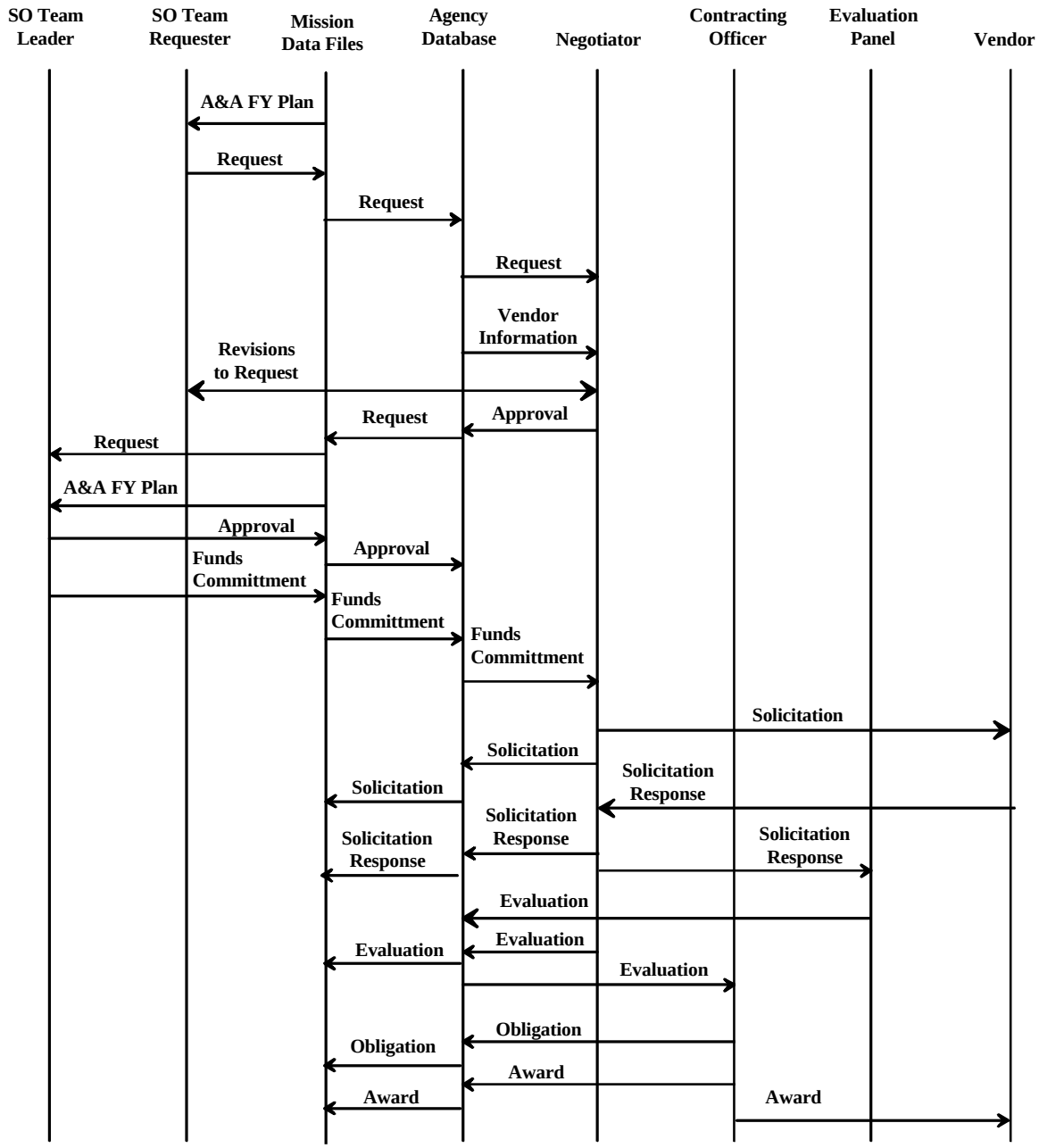



**Figure C-4. Acquisition Scenario for Hybrid Operations Concept (Contracting Officer and Negotiator in USAID/W)**

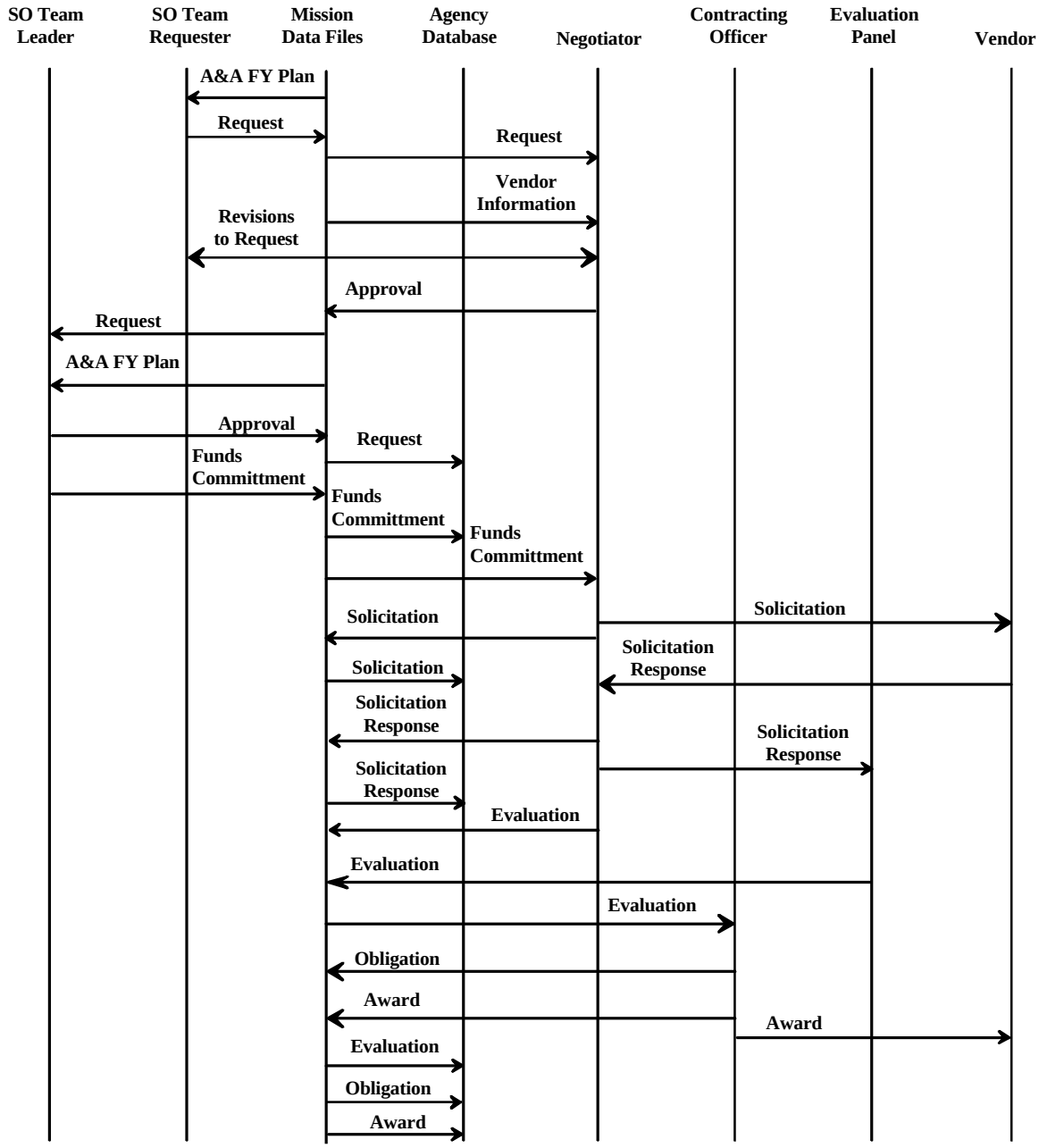



**Figure C-5. Acquisition Scenario for Hybrid Operations Concept (Contracting Officer and Negotiator in Mission)**

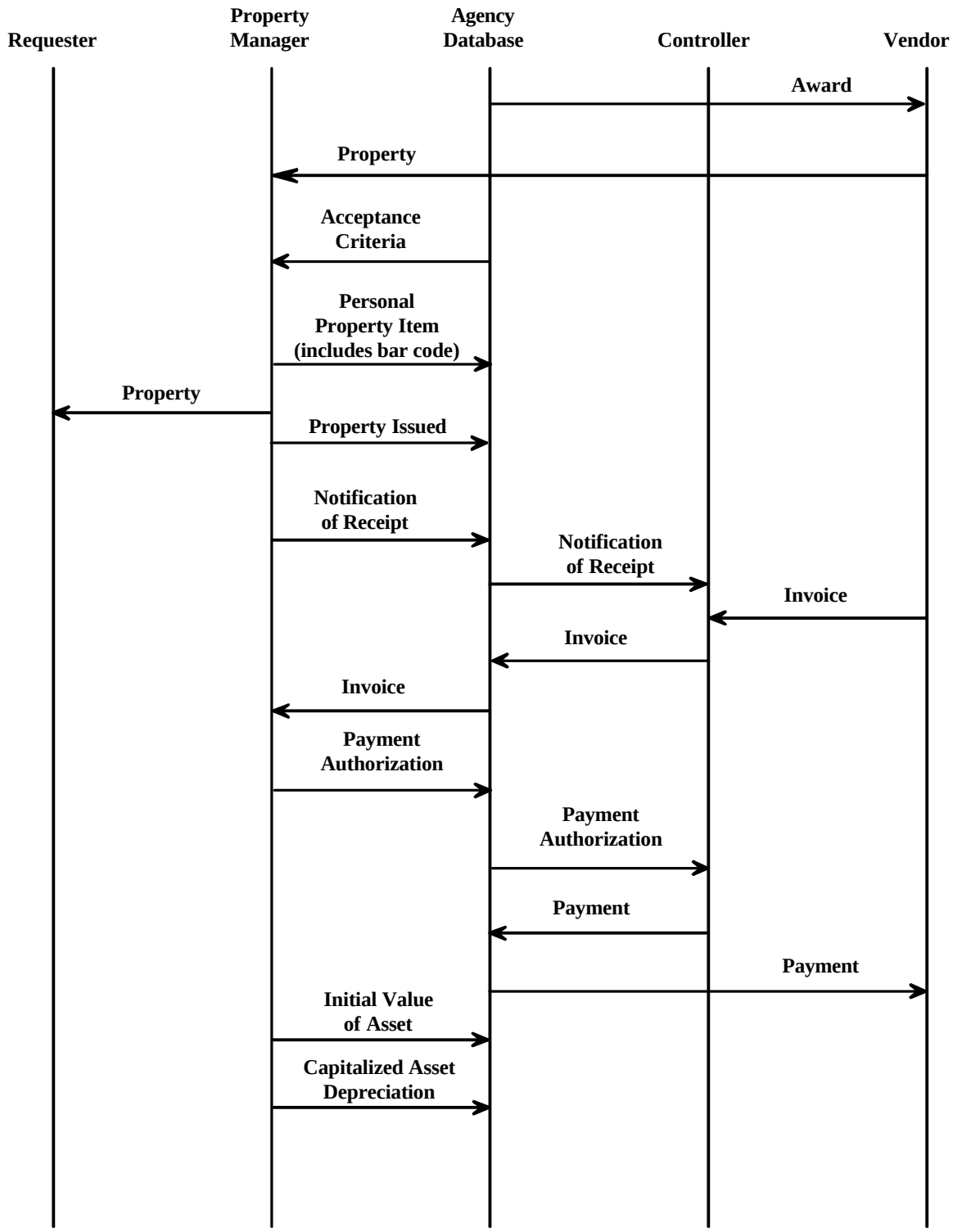



**Figure C-6. Capital Asset Property Management Scenario for Centralized Operations Concept**

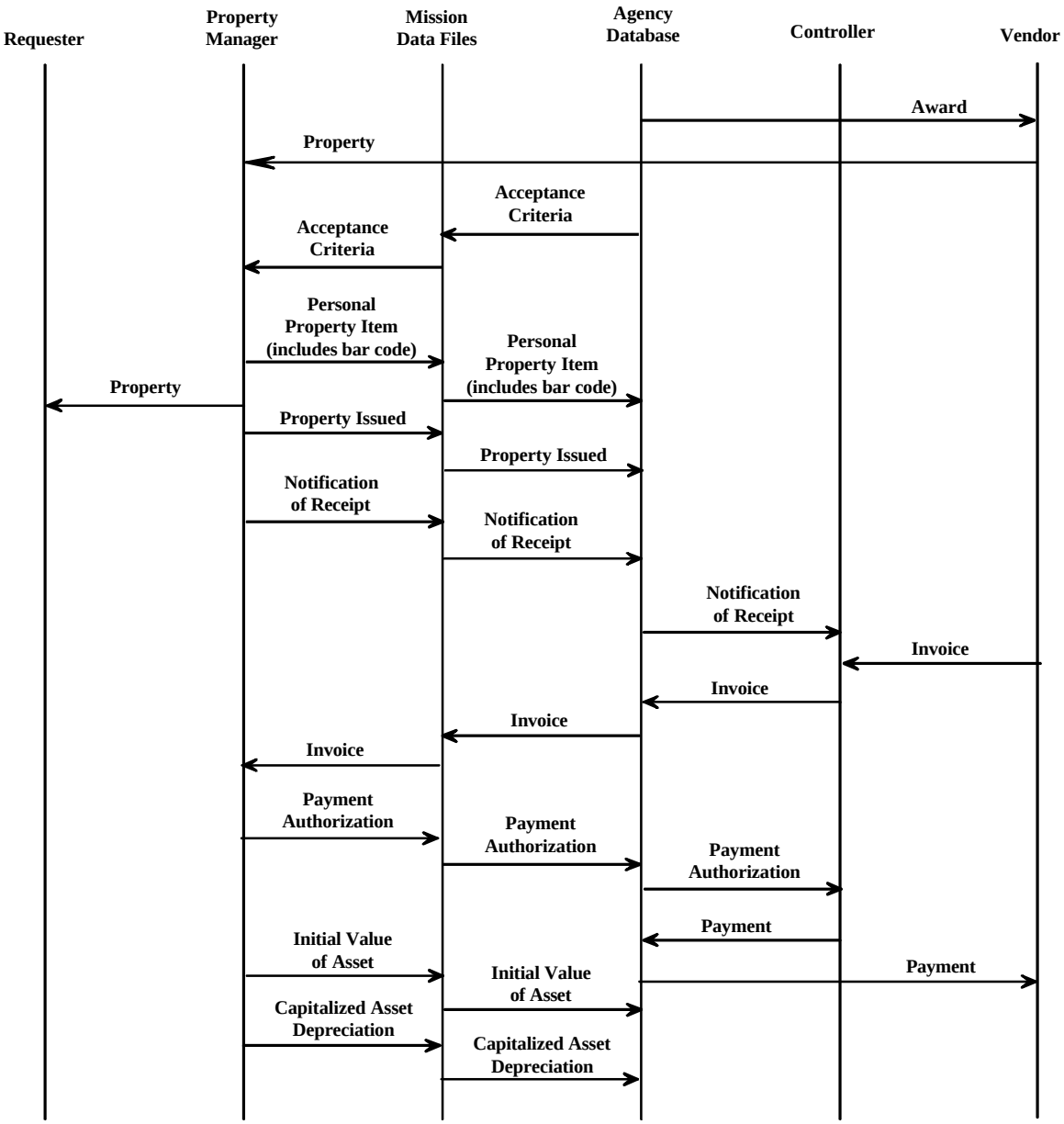



**Figure C-7. Capital Asset Property Management Scenario for Hybrid Operations Concept (Controller in USAID/W)**

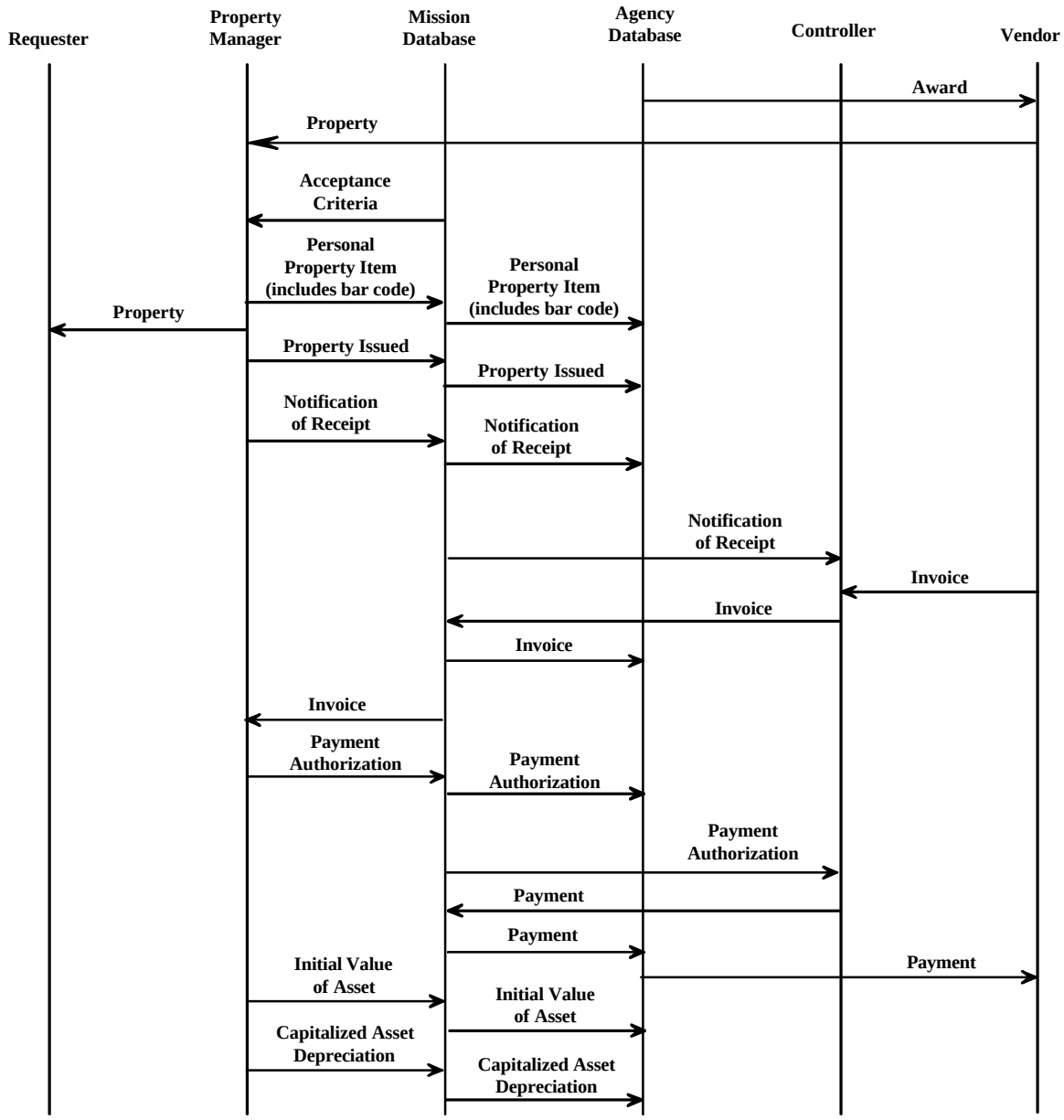



**Figure C-8. Capital Asset Property Management Scenario for Hybrid Operations Concept (Controller in Mission)**

# Appendix D. Legend for Architecture Diagrams

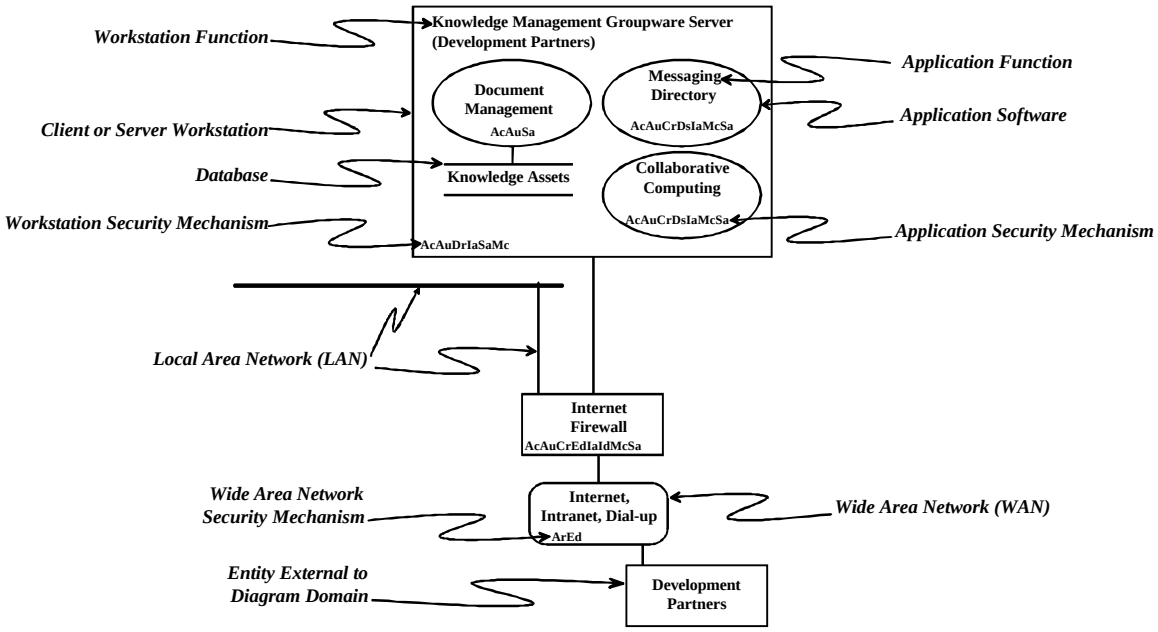



**Figure D-1. Architecture Diagram Legend**

# Appendix E. External Interface Summary Table

Table E-1 presents a summary of the interfaces between USAID business areas and external entities. The data are grouped by business area. The FROM and TO column indicate, respectively, which external entity provides and which one receives data and information to and from USAID. More detailed definitions of the USAID business areas interfaces with external entities are in the *USAID Target Enterprise Information Architecture System Requirements Report.*

**Table E-1. Summary of Business Areas Major Interfaces with External Entities (Grouped by Business Area)**

| FROM | TO | Interface definition |
|---|---|---|
| **Acquisition and Assistance** | | |
| | Vendor | 1. solicitation<br>2. award notification |
| Vendor | | 1.solicitation response<br>2. protest |
| Vendor | Vendor | Award modification/request to modify award |
| | SBA | USAID reports |
| | OMB | Reports on procurement actions |
| | Congress | Reports on Acquisition and Assistance actions |
| NIH | NIH | Contractor past performance |
| | SBA | USAID reports |
| **Budget** | | |
| OMB | | 1. OMB submission guidance and budget levels<br>2. approved apportionment |
| | OMB | 1. OMB submissions<br>2. apportionment request |
| State Department | State Department | Submit budget draft submission and<br>Receives budget submission review |
| | Congress | 1. Congressional presentation (CP)<br>2. Congressional notification (CN)<br>3. Technical notification (TN) |
| Congress | | 1. Congressional Presentation format<br>2. foreign assistance legislation<br>3. appropriation |
| U.S. Government Agencies | U.S. Government Agencies | Transferred funds and reimbursements between USAID and other U.S. Government Agencies |

| FROM | TO | Interface definition |
|---|---|---|
| **Financial Management** | | |
| | DHHS | Letter of Credit (LOC) grant transactions outsourced to DHHS (Department of Health and Human Services).<br>Current information regarding grantee: |
| DHHS | | Detailed transaction data (e.g., expenditure transaction SF272)<br>5805 Transactions<br>grant closeout information |
| | Financial Institutions | PAYLINK, automated credit card systems, Lockbox services |
| Financial Institutions | | Financial data to update payment records, record general ledger transactions; reconcile collections |
| | State Department | USDO (foreign currency payment)<br>Electronic transmission of SF 1166 Data (payment transactions and payment schedules) |
| State Department | | USDO payroll data (Used by Majority of Missions) |
| | Treasury Department | 1. GOALS reports relative to data transfer between U.S. Government agencies<br>2. ECS System data relative to payment transactions and payment schedules<br>3. Treasury/IRS 1099 data requirements<br>4. PAID data for vendors access to payment status<br>5. IGOTS data for interagency payment schedule |
| Treasury Department | | 1. GOALS updated payment status<br>2. OPAC/EDIPAC payment and collection transactions<br>3. Prime Pay (Kansas City Financial Center) disbursement transactions<br>4. TOPS data related to collections on delinquent accounts<br>5. CASHLINK collections data |
| | M&I Loan Management System | Loan obligation data. |
| M&I Loan Management System | | 1. reports for standard Credit Reform budgetary and proprietary, daily collections, and quarterly interest and fees owed. (uses interface files)<br>2. monthly manual request for advances. |
| | Vendors | USAID Web site with vendor information and payment status |
| Vendors | | 1. Electronic Data Interchange vendor invoices<br>2. USAID Document Imaging System<br>Vendor Invoices (Paper) |

| FROM | TO | Interface definition |
|---|---|---|
| Human Resources | | |
| Employee | | 1. request for status information<br>2. bids in response to a vacancy<br>3. employee input for evaluation<br>4. time and attendance<br>5. training request (SF 182)<br>6. mentor request<br>7. work objectives |
| | Employee | 1. benefit status<br>2. approval notice<br>3. placement information<br>4. midcycle evaluation<br>5. W2 forms<br>6. counseling session<br>7. learning event<br>8. assign employee (assignment: SF50)<br>9. waiver from policy or regulation<br>10. promotion nomination |
| Job Applicant | Job Applicant | advertisement,<br>application |
| State Department | | FS pay scales and FS/FSN standards |
| | Treasury Department | 1. salary and allotment,. tax, and bond information<br>2. IRS data ( Quarterly 941, W2 information) |
| | SSA | W2 payment information |
| | State Government | state tax W2 information |
| OPM | | CS standards and pay and benefits information |
| | OPM | periodic OPM reports and retirement and insurance payments |
| **Knowledge Management** | | |
| partner | | partner's development knowledge –<br>The development knowledge originated or utilized by the partner in planning and carrying out USAID program operations. This knowledge may include information contained in proposals the partner makes to USAID. |
| | U.S. Government Agencies | information for permanent government archive –<br>A subset of agency historical records provided to the National Archives for storage at designated USG repositories. |

| FROM | TO | Interface definition |
|---|---|---|
| **Program Operations** | | |
| customer | | customer needs |
| | customer | goods, services, and financial assistance (note: generally through the intermediary of partners rather than as a direct interface of USAID). |
| partner | | partner plans and capabilities, work plans, deliveries, contract review (note: USAID and the host country government negotiate a strategic objective agreement (SOAG) that is the context for the interface with partners and customers) |
| | partner | subagreement, direction |
| host country government | host country government | exchange of data, documents and information related to negotiating a strategic objective agreement (SOAG); content of the SOAG |
| **Property Management** | | |
| | GSA | SF-82 report for annual cost of USAID motor vehicle fleet. |
| | State Department | 1. Real Property Management System input<br>2. embassy space assignment<br>3. collocation waiver |
| State Department | | 1. waiver approval or disapproval<br>2. approved housing profile |
| Employee | | SF-1190 form to justify a living quarters expense that exceeds the ceiling amount. |
| U.S. Dispatch Agent | | data related to forwarding all U.S. Government property to overseas personnel |
| IAHB | IAHB | 1. to IAHB: housing profile<br>2. from IAHB: approved housing profile |
| Partner | | non-custody property to be tracked until its useful life is depleted or until contract termination |